Fehler von Fingerabdruckerkennungssystemen im Kontext

Begreifbare Vermittlung der Fehler einer biometrischen Kontrolltechnologie

Dissertation

zur Erlangung des akademischen Grades

Dr. rer. nat.
im Fach Informatik

eingereicht an der
Mathematisch-Naturwissenschaftlichen Fakultät
der Humboldt-Universität zu Berlin

von
Diplom-Informatikerin Andrea Knaut

Präsidentin der Humboldt-Universität zu Berlin
Prof. Dr.-Ing. Dr. Sabine Kunst

Dekan der Mathematisch-Naturwissenschaftlichen Fakultät II
Prof. Dr. Elmar Kulke

Gutachter/-innen:

1. Prof. Dr. Wolfgang Coy

2. Prof. Dr. Heidi Schelhowe

3. Prof. Dr. Jochen Koubek

eingereicht am: 20. Juni 2016
Tag der mündlichen Prüfung: 12. Juni 2017

Im Andenken an meinen Vater.

Zusammenfassung

In dieser Arbeit werden zwei Fragestellungen im Zusammenhang mit Fehlern von Fingerabdruckerkennungssystemen untersucht.

Erstens: Welche strukturellen Merkmale und begrifflichen Implikationen hat der spezifische Fehlerdiskurs in diesem Teilgebiet der Biometrie? Zur Beantwortung dieser Frage werden im Rahmen einer diskursanalytischen Betrachtung der Fachtexte des Forschungsfeldes die gängigen Fehlertypologien der Biometrie untersucht. Die Arbeitshypothese der Analyse ist, dass der massenhafte Einsatz von Fingerabdruckerkennungssystemen im Alltag trotz aller ihrer Fehler diskursiv durchsetzungsfähig ist. Und zwar nicht unbedingt, weil die Fehler zu vernachlässigen sind, sondern weil die Angst vor „Identitätsbetrug", die Idee einer relativ einfachen Messbarkeit von Identität und die wirtschaftliche und politische Bedeutung von Sicherheitstechniken in einer für unsicher gehaltenen Welt große Wirkmächtigkeit haben. Die besonderen Vorstellungen von der sicher feststellbaren Identität einer Person, die sich im Fehlerdiskurs niederschlagen, werden daher vertieft analysiert.

In Bezug auf die Struktur des Fehlerdiskurses wird diskutiert, inwiefern die Auseinandersetzung mit System- und Überwindungsfehlern in der Informatik zu kurz greift. Erst eine Einbeziehung der gesellschaftlichen Rolle dieser Fehler sowie die Reflexion der zugrundeliegenden Konzepte von Identität können eine prinzipielle Überprüfung des sozialen Sinns der Biometrie als Überwachungstechnik ermöglichen. Daher wird ein erweitertes Fehlermodell vorgeschlagen, das an jüngere transdisziplinäre Fehlerforschung anknüpft und als kritisches Analyseinstrument für die Beurteilung der Wechselwirkung zwischen Informatik(-system) und Gesellschaft genutzt werden kann. Es ist zudem an die Diskussionen der Implikationen, problematischen Folgen und unterschiedlichen Einschätzungen der Fehler von Überwachungstechniken in anderen Disziplinen anschlussfähig.

Zweitens: Wie lassen sich die diskursanalytische Methode und ein experimentelles, erforschendes Hands-On-Lernen zu einem Lern- und Lehrkonzept verbinden, dass eine kritische Vermittlung der Fehler und Probleme von Fingerabdruckerkennungssystemen ermöglicht? Ausgehend von schulischen Unterrichtskonzepten einer kontextualisierten, an der Lebenswelt orientierten Informatiklehre sowie der Idee des „begreifbaren Lernens" an konkreten Gegenständen wurde ein Lern- und Lehrkonzept für Universität und Schule entwickelt und in drei verschiedenen Institutionen ausprobiert. Die Ergebnisse werden ebenfalls in der Arbeit vorgestellt.

Abstract

In this paper two questions will be addressed relating to deficits in fingerprint recognition systems.

Firstly, what structural features and conceptual implications does the analysis of errors have in the field of biometrics? To answer this question, the common error types in biometrics will be examined, as part of an analytical discourse taking into consideration technical texts from the research field. The working hypothesis of this analysis is that the structure of the discourse surrounding fingerprint recognition systems would present no barriers to their widespread implementation in everyday life despite all their faults – not because their shortcomings are negligible but due to the great potency of the fear of "identity fraud", the notion that identity is relatively easy to measure, and the economic and political importance of security technologies in a world deemed unsafe. Specific notions about the guaranteed ascertainability of the identity of a person, as reflected in the error discourse, are analysed in depth.

As regards the structure of the error discourse, how the examination of system errors and spoofing attacks in computer science falls short in addressing the whole picture of failing fingerprint recognition systems will be discussed. Only by reflecting on the relevance of these errors to society and on the underlying concepts of identity can a fundamental review of the social meaning of biometrics as a surveillance technology be possible. Therefore an extended error model will be proposed, one which builds on recent transdisciplinary error research and which can be used as a critical tool for analysing and assessing the interaction between computer systems and society. It could also be tied into discussions on the implications, problematic consequences of, and different assessments of the errors of monitoring technologies in other disciplines.

Secondly, how could the analytical discourse method and experimental hands-on learning be combined into a teaching concept that would enable critical teaching of the shortcomings and problems of fingerprint recognition systems? Starting from the school-based teaching concepts of a contextualised theory of computer science based on real life and the idea of "hands-on learning" using concrete objects, a teaching concept for universities and schools has been developed and tested in three different institutions. The results are also presented in the paper.

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation

Im Januar 2003 wurde das Computersystem für den automatischen Abgleich der Fingerabdrücke von Asylbewerberinnen[1] und Illegalisierten offiziell in Betrieb genommen. Die in der Kriminaltechnik schon seit einigen Jahrzehnten angewandte biometrische Technologie wurde so erstmalig in einem supra-nationalen Kontext jenseits der polizeilichen Strafverfolgung von europäischen Staaten eingesetzt. In Pressemitteilungen und Werbebroschüren wurden Effizienz und Effektivität des Eurodac[2] genannten Systems angepriesen. Es könne rund zwei Millionen Antragstellerinnen von Einwanderungs- und Asylanträgen verwalten, rund 500.000 Vergleiche pro Sekunde durchführen und arbeite mit einer Genauigkeit von 99,9 Prozent, wie die Hersteller einzelner Komponenten angaben.[3] In der Präambel der gesetzlichen Grundlage für die Schaffung dieses Automatisierten Fingerabdruckidentifizierungssystems (AFIS) hieß es, dass Fingerabdrücke ein wichtiges Mittel zur *genauen* Identifizierung „dieser Personen“ seien und es eines Systems zum Vergleich der Fingerabdruckdaten bedürfe.[4] In der Ausschreibung der Europäischen Kommission für die Eurodac-Technik war dieses *genau* wie folgt präzisiert: „In terms of accuracy $> 99.9\,\%$ certainty for all returned submissions was a requirement with a probability of $< 0.5\,\%$ of missing a match where a match should happen.“[5] Inwiefern diese Werte für das genutzte System SteriaFIT durch Tests nach anerkannten Standards festgestellt wurden und wie hoch sie tatsächlich sind, ist in der Öffentlichkeit nicht bekannt.

Während im Gesetzestext von *genauer* Identifizierung die Rede ist, wird diese im Werbetext und in der Ausschreibung um 0,1 Prozent reduziert. Alles andere wäre unrealistisch, denn eine biometrische Mustererkennungstechnologie, wie sie ein AFIS ist, hat prinzipiell einen gewissen Prozentsatz an Falschpositiv- und Falschnegativerkennungen. Die Glaubwürdigkeit der Wirksamkeit der Technik wird also erhöht, indem die ihr innewohnende Ungenauigkeit scheinbar genau beziffert wird. Allerdings ist die Formulierung „Genauigkeit von 99,9 Prozent“ dennoch wenig aussagekräftig, da erstens nichts über die näheren Testumstände bekannt ist, die zu dieser Zahl geführt

[1] In der Arbeit wird für Personengruppen bezeichnende Substantive mal die weibliche, mal die männliche Form generisch für alle Geschlechter verwendet.

[2] Das Akronym steht für *EUROpean DACtylographic Comparison System* (vgl. European Commission 2005) und ist in Publikationen mal in der hier verwendeten, mal in Versalienschreibweise zu finden.

[3] Vgl. Haller 2004, S. 20, Steria Group Press Office 2003 sowie Cogent Systems GmbH 2003.

[4] VO (EG) 2725/2000, Erw 4.

[5] Commission of the European Communities 2004, S. 7.

haben und die nur begrenzt verallgemeinert werden können. Zum anderen reicht diese Zahl nicht aus, um eine statistisch korrekte Angabe hinsichtlich der Richtigkeit einer biometrischen Entscheidung im konkreten Szenario zu geben.

Auch in anderen EU-Verordnungen, die die Einführung biometrischer Technik im Bereich hoheitlicher Kontrollsysteme des Reiseverkehrs legitimieren, finden sich uneingeschränkt positive Aussagen über deren Zuverlässigkeit. Die Nutzung biometrischer Daten ermögliche eine „zuverlässige Verifizierung und Identifizierung von Visumantragstellern“.[6] Sie erhöhe „die Sicherheit von Reisedokumenten“, stelle „eine verlässlichere Verbindung zwischen dem Inhaber und dem Pass oder dem Reisedokument“ her und trage „damit erheblich zum Schutz vor einer betrügerischen Verwendung von Pässen oder Reisedokumenten“ bei.[7]

Biometrische Erkennungsverfahren aber sind umstrittener, als diese Formulierungen vorgeben. Dies zeigt sich nicht zuletzt an den ablehnenden Haltungen nicht-staatlicher Bürgerrechts- und Datenschutzorganisationen[8] und größeren öffentlichkeitswirksamen, aber erfolglosen juristischen Klagen gegen die Unvereinbarkeit der Passbiometrie mit den Grundrechten etwa in Deutschland und Europa.[9]

Die Gründe für die Skepsis gegenüber biometrischen Verfahren beruhen aber nicht allein auf Datenschutzbedenken, sondern auch auf der Fehlbarkeit der Systeme. So sind ihnen Systemfehler inhärent, aus denen die im ersten Absatz erwähnten Ungenauigkeiten resultieren.[10] Nie sind zwei aufgenommene Muster selbst ein und derselben Person jemals gleich.[11] Die Entscheidungsschwelle, ab der zwei Merkmale als ausreichend ähnlich gewertet werden, kann nie so eingestellt werden, dass nicht hin und wieder zwei nicht von derselben Person stammende Merkmalsmuster als gleich eingestuft werden, oder aber zwei von derselben Person stammende als unterschiedlich. Es ist also eine der bedeutendsten Herausforderungen für die Entwicklerinnen von Biometriesystemen, diese Fehler in einer Größenordnung zu halten, die in Bezug auf den Anwendungskontext vernachlässigt werden kann.

Nicht zuletzt kann biometrische Technik auf vielfältige Weise überlistet werden. Der Chaos Computer Club (CCC) demonstrierte dies in Deutschland mehrfach medienwirksam anhand der Reproduktion etwa auf Gläsern zurückgelassener Abdrücke, mit denen verschiedene handelsübliche Fingerabdruckscanner aus dem kommerziellen

[6] VO (EG) 767/2008, Erw 10.

[7] VO (EG) 2252/2004, Erw 3.

[8] Vgl. Lynch 2012; Abernathy und Tien 2003; Golembiewski und Probst 2003; CCC 2005.

[9] Vgl. BVerfG 502/09; EuGH C-291/12.

[10] „In practice, a biometric system is a pattern recognition system that inevitably makes some incorrect decisions“, heißt es bspw. bei Maltoni u. a. 2009, S. 11.

[11] Ted Dunstone und Neil Yager schreiben: „This is the origin of the probabilistic nature of biometrics, as the matching process can only give a decision confidence, not an absolute assurance […].“ (Dunstone und Yager 2009, S. 14).

Bereich leicht umgangen werden konnten.[12] Auch verschiedene Wissenschaftlerinnen im internationalen Kontext experimentierten erfolgreich mit gefälschten Fingerabdrücken.[13] Zudem konnte die Überwindbarkeit bestimmter kryptographischer Speichermethoden von Fingerabdruckdaten erfolgreich gezeigt werden.[14] Hin und wieder finden sich außerdem Zeitungsmeldungen über zufällig aufgedeckte, manchmal erfolgreiche Fälschungscoups oder Datendiebstähle.[15] Inzwischen gibt es daher systematische, gut geförderte Forschung zu Gegenstrategien,[16] getrieben von dem Motto „keeping one step ahead of the fraudsters is keeping biometrics experts on their toes".[17] Ähnliche Äußerungen über einen beständigen Wettlauf zwischen sogenannten Angreiferinnen und IT-Sicherheitsstrateginnen sind typisch im Bereich des *Security Engineering*.[18] Aus dieser Perspektive ist klar, dass es hier um einen Wettlauf mit der Kreativität der Hacker geht und vollständige Überwindungssicherheit ausgeschlossen ist.

Schließlich kann nicht bei jedem Menschen jedes biometrische Merkmal problemlos oder überhaupt gemessen werden. Einige haben aus biologischen, kulturellen oder verhaltensbedingten Gründen immer Schwierigkeiten mit der Benutzung eines biometrischen Sensors, schreiben Neil Dunstone und Ted Yager.[19] Das Merkblatt »Besonderheiten und Ausnahmen bei der Aufnahme von Fingerabdrücken« ist ein Beispiel für die entsprechenden Umgangsregelungen bei deutschen Passbehörden, falls Fingerabdrücke aus solcherlei Gründen nicht abnehmbar sind.[20]

Die Performanz-, Sicherheits- und Benutzungsprobleme für ein einzelnes System strukturiert abzuschätzen ist keine leichte Aufgabe. Biometrische Systeme sind komplexe, aus Hard- und Software-Komponenten meist verschiedener Hersteller zusammengesetzte Technologien, die nur schwierig und kostspielig zu testen sind. Unabhän-

---

[12] Vgl. starbug 2004; o. V. 2005 oder als Film vgl. CCC 2004. Siehe außerdem: o. V. 2007; erdgeist 2008; Rieger 2013; Fiebig, Krissler und Hänsch 2014.

[13] Im wissenschaftlichen Bereich vgl. u. a. Putte und Keuning 2000; Matsumoto u. a. 2002; Kaseva und Stén 2003a.

[14] Vgl. Mihăilescu, Munk und Tams 2009.

[15] Siehe zum Beispiel Columbus 2009; B. Watson 2010; Alexander 2015.

[16] Siehe bspw. Marcel, Nixon und Li 2014. Ein EU-finanziertes Projekt, zu dem einige der Buchautoren gehörten, war *Trusted Biometrics under Spoofing Attacks* (TABULA RASA). Auf einem YouTube-Kanal des Projekts lassen sich filmische Demonstrationen verschiedener üblicher Hacks unterschiedlicher Biometrie-Systeme ansehen, vgl. TABULA RASA 2013-2014.

[17] Loctier 2014.

[18] Bspw. auf der TeleTrusT-AG-Biometrie-Sitzung in der Berliner Bundesdruckerei am 16.12.2014 (Sitzungsnotizen, Knaut 2014) oder im Gespräch mit Dr. Elke Dallmer, Security Research & Consulting GmbH, Ansprechpartnerin für Sicherheitsevaluierungen im Bereich Biometrie (Gesprächsnotizen, Knaut 2015).

[19] Dunstone und Yager 2009, S. 11.

[20] Vgl. Bundesministerium des Innern 2007.

gige und detaillierte Angaben zu solchen Tests, so sie überhaupt durchgeführt wurden, für alle Produkte auf einfachem Wege zu finden, ist bis dato unmöglich.

Es kommt hinzu, dass konkrete Testdaten in Form spezifischer Fehlerraten von Teilkomponenten biometrischer Systeme, die den entsprechenden Standards genügen,[21] ohne ausreichende statistische Vorkenntnisse nur schwer einzuordnen sind. Performanzdaten zum Beispiel werden in der Regel in Form von *False Match Rate* (FMR) oder *False Non-Match Rate* (FNMR) angegeben, ablesbar an *Receiver Operation Characteristic* (ROC) *Curves* oder *Detection Error Tradeoff* (DET) *Graphs*, die zu lesen Übung erfordert.

Eine differenzierte Beurteilung der Technologien hinsichtlich ihrer Wirksamkeit und ihrer Fehler ist insbesondere für die mit ihr Erfassten und Kontrollierten – im Falle der Grenzkontrollen sind dies jeder und jede – vor diesem Hintergrund nur schwer möglich. Bedenken grundlegender Natur – etwa, welches Menschenbild hinter dem Einsatz von Biometrie steckt, inwiefern sie wirklich Sicherheit wovor bietet – können schnell als lediglich der Unkenntnis über die eigentliche Funktionsweise der Systeme geschuldet abgewiesen werden.

Die Technikerinnen, die die Systeme entwerfen, implementieren, testen oder administrieren, aber auch selbst im Alltag nutzen müssen, sind letztlich mit weit mehr als rein signalstatistischen Anforderungen konfrontiert. Im Falle der Biometrie wird, wenn sie etwa in der Migrationspolitik eingesetzt wird, der Zugang zu sozialen Ressourcen und die Einschränkung der Bewegungsfreiheit maschinell unterstützt entschieden. Der Schritt, genau hier auch Verantwortung für die oft schwerwiegenden Konsequenzen einer solchen Entscheidung dem automatisierten Verfahren zu überlassen, ist kein großer. Am Ende tragen die Informatiker damit eine sehr hohe Verantwortung. Denn sie verbürgen mit ihrer Expertise, dass die Technik in ihrem jeweiligen Anwendungsumfeld gut funktioniert und sinnvoll angepasst ist. Doch sie verweisen im Zweifel auf die Politik oder vom Kunden inadäquat formulierte Anforderungen, wenn es um vernünftige Regeln für den Datenschutz oder die Einschätzung ethischer Konsequenzen geht. Kunden oder Akteure der Politik setzen wiederum ihr Vertrauen in die Technik und übertragen die Verantwortung dorthin – ein Phänomen, das mit dem Verweis auf undurchsichtige bürokratische oder rechtliche Verfahren vergleichbar ist. Es muss daher den Entwerfenden klar sein, dass der Softwareentwurf auch eine politische Handlung ist. Um die Sinnhaftigkeit und gute Benutzbarkeit der Systeme fundiert einschätzen zu können, ist es notwendig, die ökonomischen, sozialen und politischen Prozesse, innerhalb derer sie etabliert werden, zu kennen und beurteilen zu können. Die technische als auch soziale Komplexität einer Überwachungstechnik müssen zusammen betrachtet werden. Das schließt ein, die Konzepte von Person, Identität

[21] Von der *International Organization for Standardization* (ISO) und der *International Electrotechnical Commission* (IEC) gibt es hierfür etwa die zwischen 2006 und 2012 auf sieben Einzeldokumente angewachsene Standardreihe 19795: »Biometric performance testing and reporting«.

oder Sicherheit, die das Produkt Biometrie gut verkäuflich machen, als nicht vermeintlich ausgeklammert aus der technischen Modellierung zu begreifen. Selbstverständlich ist allein das Mustererkennungsproblem „rein technisch“ oder „rein mathematisch“ interessant und schwer genug, als dass sich die Informatikerin mit dem Rest nicht unbedingt herumschlagen mag. Dennoch fehlt fast in keinem informatischen Text der Hinweis, welche Bedeutung die Biometrie in der Bekämpfung des Identitätsbetrugs, in der Erhöhung der allgemeinen Sicherheit oder als Wirtschaftsfaktor in der heutigen Welt hat – als genüge bei der forschungspolitischen Rechtfertigung eine unterkomplexe Betrachtung des Sinns und Zwecks der technischen Lösung für ein offensichtlich dann aber auch nur unterkomplex verstandenes Problem. Denn die Fehler haben in als so wichtig und bedeutsam beschriebenen politischen Problemfeldern mitunter sehr ernsthafte Konsequenzen für einzelne Betroffene und sind nicht einfach nur interessante Optimierungsprobleme. Ihre verallgemeinerte Verharmlosung ist bei deren starker Anwendungsabhängigkeit trotz allen Ärgers über kulturpessimistische Angriffe auf so interessante und ausgeklügelte Informatiksysteme, wie biometrische Anwendungen sie darstellen, fahrlässig.

Es ist daher eine grundlegende Motivation dieser Arbeit, die Fehler der *Überwachungstechnik* Biometrie in den Mittelpunkt zu stellen und herauszuarbeiten, inwiefern biometrische Systeme ein dynamischer Teil interessengeleiteter gesellschaftlicher Aushandlungsprozesse sind und wie dabei auf bestimmte mit ihr in Verbindung gebrachte Ideen von Personenidentität zurückgegriffen wird. Zudem soll nach Wegen gesucht werden, diese Aspekte erlernbar und begreifbar zu vermitteln.

1.2 Ziele & Fragestellungen

Mit der Arbeit wird das Ziel verfolgt, die *verschiedenen Darstellungen der Fehler und Probleme biometrischer Fingerabdruckerkennungstechnologien und deren Implikationen, Verflechtungen und Wirkungen systematisch herauszuarbeiten.*

Die spezielle Machtwirkung, die Biometrie-Systeme entfalten, strukturell, in ihren spezifischen Erscheinungsformen und hinsichtlich verschiedener Handlungsspielräume im Verhältnis zur fehlerbehafteten Technik zu erfassen, ist hierbei eine Maßgabe der Untersuchung. Zudem soll die Einordnung von Biometrie-Systemen als Sicherheits- oder Kontroll- und Überwachungstechnologie hinsichtlich der verschiedenen institutionellen, technikbedingten und individuellen Sichtweisen vorgenommen werden.

Der Untersuchung wird eine Arbeitshypothese vorangestellt, die im Zuge der ersten Recherchen zu dieser Arbeit entstanden ist. Sie leitet sich zum einen aus allgemeinen Beobachtungen der *Surveillance Studies* ab, wie sie etwa David Lyon konzeptionalisiert hat[22] und wie sie in Foucaults Sicherheitsdispositiv vorgedacht sind: Dazu gehören das

[22] Vgl. Lyon 2002.

auf alle verallgemeinerte Verdachtsmoment und die Notwendigkeit, die Risiken, die Personen für eine Gesellschaft beziehungsweise deren *Sicherheit* darstellen, möglichst automatisch zu klassifizieren. Der menschliche Körper erzeugt Daten, die eine solche Klassifikation ermöglichen – es gibt eine Fixierung des Risikos an das Äußere, Messbare, das abstrahiert wird („phenetic fix"). Zum anderen folgt die Arbeitshypothese der Beobachtung, dass mustererkennende Sicherheitstechnologien das Problem, das sie bekämpfen sollen, nie vollständig lösen können und zudem ihre Profitabilität von dessen Weiterbestehen abhängt. In dieser Arbeit wird dies speziell anhand biometrischer Fingerabdruckerkennungstechniken untersucht. Die Arbeitshypothese wird nach der ausführlichen Analyse abschließend erstens darauf geprüft, inwiefern sie eine sinnvolle Erklärung für die Weiterentwicklung unsicherer Sicherheitstechnologien bietet und zweitens, inwieweit sie sich auf alle Biometriesysteme oder gar Überwachungs- bzw. Sicherheitstechnologien verallgemeinern lässt:

Diskursiv sind Fingerabdruckerkennungssysteme trotz aller Kritik durchsetzungsfähig und ihre Fehler werden als zu vernachlässigende angesehen. Dies geschieht aufgrund einer geschichtlichen, ökonomischen, sozialen und politischen Konstellation, in der

(a) „Identitätsbetrug" als allgegenwärtige und akute Bedrohung gilt – jede Person ist dieser Tat prinzipiell verdächtig –,

(b) Identität als an den Körper gekoppelte Unveränderlichkeit der Person gesehen wird, die messbar und somit als Datum digitalisierbar ist, und

(c) die stetige Anpassung und Verbesserung einer *fast* sicheren Technologie ein erhebliches wirtschaftliches Wachstum generiert.

Dies spiegelt sich in der biometrischen Fachliteratur wider.
Kurz: Wie gut die Systeme real funktionieren, ist für ihre Durchsetzung zweitrangig.

Um dieser These auf den Grund gehen zu können, werden sowohl Fachpublikationen der Informatik als auch der Sozial- und Geisteswissenschaften unter dem Gesichtspunkt analysiert, wie darin die Fehler biometrischer Systeme dargestellt werden und was über ihre Vermittlung an Nutzerinnen gesagt wird.

Aufbauend auf den Erkenntnissen der vorhergehenden Analyse werden *Überlegungen zu einer kritischen Vermittlung der Fehler und Probleme von Fingerabdruckerkennungssystemen im Rahmen eines Bildungskonzepts* vorgestellt. Hierbei sollen historische, sozialwissenschaftliche und technische Herangehensweisen didaktisch sinnvoll integriert werden. Es werden Ansätze beschrieben, mittels derer sowohl die stochastischen Vorgänge der Mustererkennung als auch die Einbettung eines solchen Systems in einen sozialen Kontext veranschaulicht werden können.

Als konkretes Beispiel wird ein Bildungskonzept entworfen, das auf diskursanalytische sowie praktische Elemente zurückgreift, um biometrische Systeme kritisch, fehlerzentriert und experimentell zu erschließen.

1.3 Vorgehen

Der Untersuchungsgegenstand der Arbeit beschränkt sich auf automatisierte Fingerabdruckerkennungssysteme als bereits seit vielen Jahrzehnten in der Kriminalistik und seit Ende der 1990er in hoheitlichen Massenanwendungen und im privatwirtschaftlichen Anwendungskontext etablierte Technologie.

Zur genaueren Eingrenzung der Forschungslücke wird nach Einführung in die Grundlagen der biometrischen Fingerabdruckerkennung sowie die damit zusammenhängenden Fehlerbegriffe eine vertiefte Analyse der technischen unter Einbeziehung sozial- und geisteswissenschaftlicher Fachliteratur durchgeführt. Die Leerstelle vermute ich hier in einer bisher fehlenden informatischen Perspektive, die eine Manifestierung von Begriffs(-miss-)verständnissen, Interessen und Machtverhältnissen zwischen verschiedenen Akteursgruppen in der Beschreibung der Fehler biometrischer Fingerabdrucksysteme und vor allem ihrer Vermittlung an unterlegene Nutzerinnen integriert und dabei auch soziokulturelle Aspekte mit einbezieht. Die Untersuchungen der eher disparaten und nicht in Dialog gebrachten Einzelsichten werden für die Erarbeitung aber zunächst in ihren jeweiligen Rahmen betrachtet.

In der inhaltlichen Analyse betrachte ich das, was in verschiedenen wissenschaftlichen Publikationen über Fehler biometrischer Fingerabdruckerkennungssysteme gesagt wird, als Teil eines *Fehlerdiskurses*. Der Begriff *Diskurs* – etymologisch laut Duden: „lateinisch discursus = das Sich-Ergehen über etwas, das Auseinander-, Umherlaufen“[23] – wird sehr häufig benutzt, um Debatten oder Sprechweisen innerhalb bestimmter thematischer Kontexte zu beschreiben. Mittels Diskursen als „Äußerungszusammenh[ä]ng[en]“[24] lässt sich der gesellschaftliche Verwendungs- und Herstellungskontext einer Technik erschließen. Er wird beobachtbar anhand seiner „medialen Aufbereitungen […], die als Dokumente, Artikel, Kommentare, audiovisuelle Beiträge, Webseiten etc. zu Themen geordnet, diskutiert, ausgehandelt und vermittelt werden.“[25] Dementsprechend reiht sich die Analyse des Diskurses in die Vielfalt methodologischer Möglichkeiten ein, eine „Hermeneutik von Verstehens- und Verständigungsakten“[26] innerhalb der Technikwissenschaft zu entwickeln. Im von Dirk Siefkes, Peter Eulenhöfer, Heike Stach und Klaus Städtler 1998 herausgegebenen Buch »Sozialgeschichte der Informatik« werden Diskurs, Denkraum und Praktiken als Begriffstrias benutzt. Sie konstituieren das „Sprach-, Wissens- und Technikfeld[…], das die neue Technik von Beginn an mit Sinn und Bedeutung versah“.[27]

---

[23] http://www.duden.de/rechtschreibung/Diskurs, letzter Abruf: 22.7.2017.

[24] Koubek, Schulte u. a. 2009, S. 272.

[25] Ebd. Wie dies im Schul- oder Hochschulkontext didaktisch umgesetzt werden kann, wird in Unterkapitel 5.1.1 genauer ausgeführt.

[26] Hellige 1996, S. 15.

[27] Siefkes u. a. 1998, S. 7.

In der vorliegenden Untersuchung soll mittels kritischer Inhaltsanalyse in der Erarbeitung des Forschungsstands als relevant herausgearbeiteter Texte die Synthese der verschiedenen Darstellungen der Fehler biometrischer Fingerabdruckerkennungssysteme in einem „Fehlerdiskurs" aufgezeigt und in einer für diese Arbeit entwickelten Taxonomie angeordnet werden. Hierbei sehe ich Diskurse im Sinne der Kritischen Diskursanalyse.[28] Sie setzt am Diskursbegriff Foucaults an. Bei Foucault sind Diskurse „transsubjektive Produzenten gesellschaftlicher Wirklichkeit und sozio-kulturelle Deutungsmuster".[29] Mit ihnen wird historisch und räumlich jeweils gültiges Wissen zwischen Menschen transportiert, und sie können Verhalten und andere Diskurse induzieren und sind damit ein Machtfaktor.[30] Während der Diskursbegriff auf sprachlich-schriftliche Aussagen beschränkt ist, erweitert der Begriff des Dispositivs diesen um vergegenständlichte, bildliche oder andere sinnliche Praktiken sowie konkrete Handlungen, in denen sich das diskursive Wissen artikuliert.[31] In Bezug auf Technik lässt sich das Dispositiv im Sinne des Latourschen Satzes „Technik ist stabilisierte Gesellschaft" verstehen.[32] Das heißt zum Beispiel, dass bestimmte Systemkomponenten durch ihre technische Konfiguration und ihr Interface-Design die möglichen Interaktionen mit anderen Systemkomponenten oder Menschen determinieren und ihnen der Diskurs eingeschrieben ist.

In der Kritischen Diskurs- und Dispositivanalyse geht es also um die Beschreibung der sprachlichen, handlungskennzeichnenden und gegenständlichen Muster einer gesellschaftlichen Auseinandersetzung um ein bestimmtes Thema – in dieser Arbeit sind dies die Fehler von automatischen Fingerabdruckerkennungssystemen. Ziel ist es, „das **Wissen** bzw. die **Aussagen** zu eruieren, die die jeweiligen „Kulturen" und all ihre Erscheinungsformen/Positivitäten leiten."[33]

Zur textlichen Materialbasis für die Betrachtung gehören deutsch- und englischsprachige fachwissenschaftliche Veröffentlichungen, Publikationen der Biometrie-IT-Branche (Pressemitteilungen und Produktinformationen), relevante Standards der *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC), amerikanischen sowie deutschen Standardisierungsgremien, Berichte von Multi-Stakeholder-Zusammenschlüssen für die Biometrie, Notizen aus Gesprächen mit verschiedenen Expertinnen in der Biometrie sowie ausgewählte Pressemeldungen in Special-Interest-Medien (z. B. verschiedene heise-Medien, Wired, o. ä.) rund

[28] Die Kritische Diskursanalyse, die Siegfried Jäger im gleichnamigen Buch beschreibt, wurde seit Anfang der 1990er Jahre am Duisburger Institut für Sozialforschung entwickelt und in den letzten Jahren um die Dispositivanalyse erweitert. Vgl. S. Jäger 2012.

[29] Ebd., S. 26.

[30] Vgl. ebd., S. 38.

[31] Vgl. ebd., S. 226.

[32] Latour 2006.

[33] S. Jäger 2012, S. 76, Hervorhebung im Original.

um Fehler von Fingerabdruckerkennungssystemen vor allem der letzten beiden Jahrzehnte und schließlich Soft- und Hardware realisierter Fingerabdruckerkennungssysteme. Der Blick auf die Biometrie aus den Geistes- und Sozialwissenschaften wird in Teilen ebenfalls mit einbezogen. Während das verschriftlichte Material Teil des Diskurses ist, sind die biometrischen Systeme zwar teils als Code und dessen Dokumentation verschriftlicht, aber durch ihre Schnittstellen und konkrete Hardware-Beschaffenheit auch vergegenständlicht und damit Dispositive.

Eine strukturelle Analyse, über welche Arten von Fehlern welche *Aussagen*, die nach Foucault die „Atome oder auch Kerne des Diskurses" darstellen,[34] getroffen werden und auf welche Weise diese getroffen werden (grafische Gestaltung, Themen, Quellen, Kollektivsymbolik, Diskursposition, sprachlich-rhetorische Mittel und inhaltlich-ideologische Aussagen, Besonderes, etc.), wird anhand ausgewählter thematischer Diskursfelder vorgenommen. Sie gruppieren bestimmte Aussagenkomplexe, die sich bei der Lektüre der Publikationen des Forschungsstandes als auffällig häufig herausstellen. Außerdem gehört die Benennung zentraler Akteure in ihrem institutionellen Kontext, die zum Fortgang des Diskurses auf verschiedene Weise und aus verschiedenen Machtpositionen heraus beitragen, ebenfalls dazu.

Die gesamte Analyse soll Rückschlüsse auf die eingangs gesetzte These ermöglichen, nämlich, dass von geringer Relevanz ist, wie gut die Fingerabdruckerkennungssysteme funktionieren, da sie diskursiv aus anderen Gründen durchsetzbar sind.

Ein weiterer wichtiger Teil dieser Arbeit ist es, das Vorgehen der kritischen Analyse eines biometrischen Fingerabdruckerkennungssystems auf die Informatikdidaktik zu übertragen. Es soll anhand verschiedener umgesetzter Lehr- und Lernszenarien gezeigt werden, wie eine kontextualisierte Analyse von Informatiksystemen im Rahmen einer ganzheitlichen Informatikausbildung eingesetzt werden kann. Die Konzeptualisierung konkreter Lehr- und Lernszenarien wird dabei an den informatikdidaktischen Überlegungen orientiert, die Ende der Nullerjahre in das Planungs-, Durchführungs- und Auswertungskonzept »Informatik im Kontext« mündeten.[35] Hierin stellt sich der Bezug zum informatischen Lerngegenstand vor allem über die unmittelbare alltägliche Betroffenheit der Lernenden her (Lebenswelt)[36] und tangiert verschiedene gesellschaftliche Dimensionen (Mehrdimensionalität). Bei Biometriesystemen gibt es zum einen eine beständig wachsende Zahl alltäglicher Anwendungen wie die Authentifizierungssysteme an Smartphones oder Laptops oder die Gesichts- und Fingerbilder

[34] Ebd., S. 95.

[35] Ideen, „Informatikunterricht […] mit den Alltagserfahrungen einer lebendigen Technik im gesellschaftlichen Kontext zu vermitteln" (Coy 2005), wurden in diesem Konzept von Schul- und Hochschullehrern gleichermaßen systematisch zusammengeführt (vgl. Koubek, Diethelm und Witten 2011, S. 97 ff.).

[36] Die im Rest des Absatzes in Klammern genannten Kriterien für ein geeignetes Informatik-im-Kontext-Thema stammen aus ebd., S. 102 f.

für diverse Ausweise. Zum anderen sind vielfältige rechtliche, kulturelle oder wirtschaftliche Dimensionen von großer Relevanz für die Ausgestaltung und die Auswirkungen der Systeme. Der Biometrie-Kontext lässt sich nicht allein rein mathematisch-technisch erschließen (Breite). Dennoch ist zu seinem Verständnis ein „solides Hintergrundwissen aus der Informatik nötig, um die Phänomene, die den Kontext ausmachen, zu verstehen. Anzeichen für die fachliche Tiefe sind die enge Verknüpfung des Kontexts mit informatischen Fachbegriffen und Grundprinzipien“ (Tiefe).[37] Mustererkennung, Signalverarbeitung und Maschinelles Lernen sind die wichtigsten informatischen Gebiete, aus denen das Hintergrundwissen für die Biometrie stammt. Schließlich hat das erworbene Wissen über den soziokulturellen Problembereich der Personenerkennung anhand körperlicher Merkmale, ihrer Implikationen und Anforderungen, seiner Übersetzung in fehlerbehaftete technische Lösungen als Teil politischer Aushandlungen sowie das Wissen über die konkreten mathematisch-technischen Formalisierungen derselben über einen langen Zeitraum Bestand (Stabilität).

Das im Rahmen dieser Arbeit entwickelte Lern- und Lehrkonzept ist allerdings nicht streng an dem oben genannten Schema orientiert, sondern etwas offener angelegt und um Hands-on-Lernen ergänzt, das im Sinne eines be-greifenden Lernens verstanden werden kann.[38] Erst in Verbindung mit einer direkten praktischen, spielerischen und experimentierenden Auseinandersetzung mit den konkreten Komponenten des Biometrie-Systems werden die Texte über die Systeme greifbar. Das Über-die-Technik-Erzählte, sei es in den Konzernwerbungen, in den Überlistungs- oder Benchmark-Tests oder in den wissenschaftlichen Veröffentlichungen, kann in Beziehung zu ihr selbst gesetzt und an ihr geprüft werden – dies begleitende Fragen sind zum Beispiel: Lassen sich kommerzielle Fingerabdruckscanner wirklich so leicht austricksen, wie in unterschiedlichen Kontexten berichtet? Wie nachvollziehbar und reproduzierbar ist ein Performanztest am konkreten Gerät? Wie sind die Erkennungs- und Vergleichsalgorithmen konkret implementiert, wie die Schnittstellen? Welche Rahmenbedingungen müssen jeweils erfüllt sein? Wie dokumentiert ein Hersteller seine Software? Ist sie quelloffen? Wie ist das *User Interface* gestaltet? Wie modular ist das System?

Parallel und als Teil der Konzeptionierung werden praktische Unterrichts- bzw. Seminarprojektversuche durchgeführt und dokumentiert.

[37] Koubek, Diethelm und Witten 2011, S. 102.

[38] Dies schließt sich an den Ansatz von Bernard Robben und Heidi Schelhowe an, siehe Robben und Schelhowe 2012.

1.4 Aufbau

Die Gliederung der Arbeit orientiert sich an den eingangs erläuterten Thesen und Fragestellungen und dem gewählten Vorgehen zu ihrer Beantwortung:

- In *Grundlagen und zentrale Begriffe* (Teil 2) werden Definitionen der Grundbegriffe der informatischen Biometrie vorgestellt sowie Funktionsweise und Aufbau eines biometrischen Systems allgemein erläutert. Da es hier zunächst darum geht, ein grundlegendes Verständnis biometrischer Fingerabdruckerkennungssysteme zu ermöglichen, wird hier noch nicht begriffskritisch gearbeitet, sondern zunächst die Darstellung des Wissensgebietes mit Rückgriff auf wenige Grundlagenwerke und gegenwärtige ISO/IEC-Standards umrissen.

  Außerdem wird der für diese Arbeit als Analysekategorie verwendete Begriff des Fehlers definiert und in verschiedene Teilkategorien zerlegt.

- Ein Überblick über die Fehlerforschung in der Biometrie sowie anderer Disziplinen bezüglich der Biometrie findet sich in *Forschungsstand: Fehler von Fingerabdruckerkennungssystemen* (Teil 3).

- Im Kapitel *Ausgewählte Diskurse um Fehler von Fingerabdruckerkennungssystemen* (Teil 4) werden einige auffallende Strukturmerkmale und Erscheinungsformen des Fehlerdiskurses der im Forschungsstand besprochenen technischen Publikationen herausgearbeitet und analysiert.

- Das Kapitel *Didaktische Aufbereitung – Biometrische Fingerabdruckerkennung im Kontext* (Teil 5) zeigt, wie eine kontextualisierte kritische Erschließung vorhandener Fingerabdrucktechnologien und ihrer Fehler als Teil der Informatik-Lehre an Schule oder Hochschule aufbereitet werden könnte. Konkret durchgeführte Versuche und ihre Konzepte werden vorgestellt sowie methodische Erweiterungen vorgeschlagen.

- Im *Schluss* (Teil 6) wird schließlich die eingangs aufgestellte These anhand der Ergebnisse der Diskursanalyse diskutiert. Zudem wird resümiert, wie sich die Ergebnisse der didaktischen Umsetzung diskursanalytischer Ansätze in Bezug auf den Untersuchungsgegenstand – biometrische Fingerabdruckerkennungssysteme – dazu verhalten.

2 Grundlagen und zentrale Begriffe

Dieser Teil ist in sechs Kapitel gegliedert. Im Kapitel *Historischer Hintergrund* (2.1) werden die allgemeine disziplinäre Verankerung der Biometrie innerhalb der Wissenschaften und erste wichtige Grundbegriffe der Fingerabdruckerkennung in einem knappen geschichtlichen Kontext erläutert. Weitere grundlegende Definitionen und Konzepte folgen dann im Kapitel *Grundbegriffe biometrischer Systeme* (2.2). Daran schließen sich im Kapitel *Allgemeine Systemarchitektur biometrischer Systeme* (2.3) wichtige Begrifflichkeiten zur Beschreibung der generischen Systemarchitektur eines biometrischen Systems und seiner Funktionsweise an. Auf die zugehörigen Prozesse wird etwas ausführlicher im Kapitel *Prozesse in biometrischen Systemen* (2.4) eingegangen. Die Ausführungen im Kapitel *Fehlerbegriffe* (2.5) beleuchten dann die verschiedenen Perspektiven auf Fehler biometrischer Systeme, die für die Bearbeitung des Themas der Arbeit eingenommen werden. Schließlich rundet ein kurzes Resümee (2.6) des Begriffskapitels den gesamten Einstiegsteil ab.

Als vornehmliche Quellen des zweiten, dritten und vierten Kapitels dienen das harmonisierte biometrische Vokabular der *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC) und das für die Fingerbild-Biometrie wichtige Grundlagenwerk »Handbook of Fingerprint Recognition« von Davide Maltoni, Dario Maio, Anil K. Jain und Salil Prabhakar, die nicht an jeder Stelle explizit angegeben sind.[39] Weitere Quellen werden stets direkt genannt.

2.1 Historischer Hintergrund

2.1.1 Entstehung der informatischen Biometrie

Seit mehr als 100 Jahren wird die biologische oder medizinische Statistik als *Biometrie* (auch: *Biometrik*; engl.: *Biometrics* oder selten: *Biometry*) bezeichnet. Sie entstand im Zuge der Entwicklung mathematischer Methoden zur Erfassung und Analyse biologischer und medizinischer Artefakte und Prozesse.

Der Statistikhistoriker Stephen M. Stigler schreibt, dass die wissenschaftliche Disziplin Biometrie vor allem auf zwei noch heute bestehende Zeitschriften zurückgeht:[40] Eines ist das 1901 von Francis Galton, Karl Pearson und anderen gegründete Journal »Biometrika«, das anfangs hauptsächlich die Anwendung statistischer Verfahren zur Beforschung von Vererbung und Evolution thematisierte.[41] Das andere ist das 1945

[39] Siehe ISO/IEC 2382-37:2017 und Maltoni u. a. 2009.

[40] Vgl. Stigler 2000, S. 657.

[41] Vgl. ebd., S. 653.

gegründete und heute von der traditionsreichen *International Biometric Society* (IBS) herausgegebene Journal »Biometrics« (ursprünglich »Biometrics Bulletin«).

Die statistisch fundierte Vermessung insbesondere des menschlichen Lebens innerhalb der Biologie und der Medizin ging einher mit einer sich zunehmend auf Empirie berufenden Nationalökonomie und Staatswissenschaft.[42] Christel Weiß verweist in diesem Zusammenhang auf die lange Tradierung statistischer Erfassung im staatlichen Kontext Europas. Dazu gehören zum Beispiel Volkszählungen seit dem Altertum, Geburten- und Sterberegister der Kirchen ab dem 16. Jahrhundert sowie die „politische Arithmetik" im England des 18. Jahrhunderts.[43] Sie erwähnt, dass der im 18. Jahrhundert in Göttingen lehrende Staatswissenschaftler Gottfried Achenwall den Begriff „Statistik" eingeführt hat und ihn „gleichbedeutend mit ‚Staatsbeschreibung' verwendete". So leite sich die „Wurzel der beiden Wörter ‚Staat' und ‚Statistik' […] vom lateinischen ‚status' (Zustand, Beschaffenheit)" her.[44] Zudem gingen, ab dem 18./19. Jahrhundert in England beginnend, bevölkerungsstatistische Untersuchungen mit der beginnenden Hygienebewegung und den „Ansätze[n] zu einer Kollektivmedizin, die etwa gute Wasserversorgung und prophylaktische Maßnahmen für breite Bevölkerungskreise als Schutz gegen Krankheiten" beinhaltete, einher.[45] Es konstituierte sich letztlich eine Bevölkerungswissenschaft (Demographie), die in enger Wechselwirkung mit der Verwissenschaftlichung von Medizin und Biologie stand.[46] In diesem Kontext war die Demographie auch zentraler Bestandteil der Eugenik, die Ende des 19. Jahrhunderts/Anfang des 20. Jahrhunderts einen enormen Aufschwung hatte – sowohl Galton als auch Pearson waren überzeugte Eugeniker – und bis hin zur nationalsozialistischen Rassenlehre führte.[47] Gleichermaßen wirkte sie hinein in die biologische und forensische Anthropologie sowie die Kriminalbiologie und die Kriminalistik.[48] Insbesondere

[42] Vgl. Weiß 2005.

[43] Ebd., S. 3. Zur Rolle, die der in den Registraturen niedergeschriebene Geburtsname dabei bekommt und wie er zum Herrschaftsinstrument wird, siehe auch Engemann 2013.

[44] Weiß 2005, S. 3.

[45] Ebd., S. 6 f.

[46] Zur kritischen Geschichte der Bevölkerungswissenschaft, in der auch ihre Verkettung mit Eugenik und Rassenlehre thematisiert wird, siehe bspw. Mackensen 2002 und Mackensen 2006. In der Arbeit zum „Bevölkerungsdiskurs" von Hummel 2000 wird zudem der Foucaultsche Begriff der Biomacht und der damit zusammenhängende der Biopolitik in eine Kritik der Demographie einbezogen.

[47] Siehe hierzu auch Mackensen und Reulecke 2005 – im Sammelband finden sich Aufsätze zum Zusammenhang von Eugenik und Bevölkerungswissenschaft in Deutschland (Kröner, in: Ebd., S. 429 ff.), zu den Begriffen *Eugenik* und *Rassenhygiene* in der Rezeption der Mediziner und Biologen Anfang 20. Jh. (Petermann, in: Ebd., S. 433 ff.), zur Konstruktion des Eigenen und des Fremden in bevölkerungswissenschaftlicher Grundlagenforschung um 1933 (Haar, in: Ebd., S. 340 ff.) sowie zur Rolle der Anthropometrie in der biologistischen Stadtforschung Ende 19. Jh. (Ferdinand, in: Ebd., S. 124).

[48] Vgl. bspw. Vec 2001 zur Rolle der biometrischen Körpervermessung für die Kriminalistik und Kriminalanthropologie.

in der Kriminalistik wurden die auch in der rasse- und erbbiologischen Forschung verwendeten Methoden wie die Daktyloskopie oder das anthropometrische System von Alphonse Bertillon dahingehend entwickelt,[49] Individuen in anonymen gesellschaftlichen Kontexten verlässlich wiederzuerkennen. Im Zuge der Automationsmöglichkeiten, die sich mit der Computerisierung boten, wurden diese Methoden für die maschinelle Nutzung angepasst. Die hiermit einhergehende Forschung zur automatischen Personenwiedererkennung hat sich hernach als eine spezielle, eigenständige Richtung der Biometrie entwickelt.[50]

Von diesem „aufkommenden Gebiet einer Technologie, die sich der Identifizierung von Individuen mittels biologischer Merkmale widmet, wie zum Beispiel jene, die auf Retina- oder Irisscanning, Fingerabdrücke oder Gesichtserkennung gegründet“ seien, grenzt sich die IBS jedoch deutlich ab.[51] Weder das Journal »Biometrics« noch der Verband selbst seien an Forschung, Marketing oder Berichterstattung in Bezug auf diese Technologie beteiligt. Dennoch haben die beiden Gebiete nicht nur ihren Namen gemein, sondern sind, bezogen auf die Vermessung von biologischen Phänomenen, miteinander verwandt und greifen auf ähnliche Teilgebiete der Informatik zurück.

Biostatistikerinnen verfügen inzwischen über ein technisches Arsenal, das nur noch wenig mit der Biometrie Anfang des 20. Jahrhunderts gemein hat.[52] Hierzu gehört inzwischen auch die Bioinformatik. Als eigenständige Studiendisziplin ist sie mit der Datenhaltung und -analyse verschiedener riesiger biologischer Datenmengen in Hinblick auf Aussagen und Erkenntnisse im Bereich evolutionsbiologischer Fragestellungen befasst und stellt eine Automatisierung und Erweiterung der Biometrie als Methodologie der Medizinischen und Biologischen Statistik dar.

Biometrie im Sinne dieser Arbeit könnte auch als ein kleiner Anwendungsbereich eben dieses Gebiets betrachtet werden. Gleichzeitig widerspricht diese Sicht aber eher dem Selbstverständnis derjenigen, die Biometrie als automatisierte Identifizierungstechnik, manchmal sogar als eigene Wissenschaft der Identifizierung betrachten.[53] Ich

---

[49] Zur als Daktyloskopie bezeichneten Fingerabdruckidentifizierung siehe *Unterkapitel 2.1.2 Manuelle Fingerabdruckerkennung* (S. 28). Das anthropometrische System der sogenannten Bertillonage war um 1880 entwickelt worden und diente zur Vermessung verschiedener Körperteile von Menschen zum Zwecke ihrer Identifizierung – vgl. ebd.

[50] Sie hat sich bisher allerdings nicht in dem Maße wie die Bioinformatik als wissenschaftlich eigenständige Disziplin entwickelt; zur Herausbildung von Studiengängen, Instituten oder Lehrstühlen für informatische Biometrie siehe Kapitel 3.7.

[51] Vgl. International Biometric Society o. J. Von Verfasserin übersetzt.

[52] Vgl. Stigler 2000, S. 657.

[53] So definieren etwa die Informatiker Ruud Bolle et al.: „[…] biometrics is the science of identifying, or verifying the identity of, a person based on physiological or behavioral characteristics.“, Bolle u. a. 2004, S. 3. Mehr zu den Biometrie-Definitionen im *Unterkapitel 2.2.1 Biometrie und ihre Definitionen* (S. 32).

werde sie zur klaren Abgrenzung von der Biostatistik in dieser Arbeit manchmal auch als *informatische Biometrie* bezeichnen.[54]

Die informatische Biometrie bedient sich weitestgehend der Verfahren, die in den Teilgebieten *Signalverarbeitung* (*Signal Processing*),[55] speziell auch *Bildverarbeitung* (*Image Processing*), *Mustererkennung* (*Pattern Recognition*) und *Maschinenlernen* (*Machine Learning*) verankert sind.[56] Die Automatisierung der Fingerabdruckerkennung war die erste bedeutende Aufgabe der informatischen Biometrie – dieser Bereich hat sich über viele Jahrzehnte inzwischen fest etabliert.

2.1.2 Manuelle Fingerabdruckerkennung

Die kriminalistische Daktyloskopie, also die „Fingerschau" zur Identifizierung Tatverdächtiger,[57] ist seit gut einem Jahrhundert eine gängige polizeiliche Praxis. Dabei werden auf Gegenständen hinterlassene Fingerabdrücke, also die charakteristischen von den Hautleisten (*Papillarlinien*/*Ridges*) an den oberen Innenseiten der Finger zurückgelassenen Spuren, mit von Tatverdächtigen oder als Straftäterinnen verurteilten Personen bei der Polizei abgenommenen Fingerabdrücken verglichen. Auch Handflächen, die Fußspitzen und Fußunterseiten besitzen diese charakteristischen Abdrücke und werden gegebenenfalls, aber seltener auch zur Identifizierung genutzt – in der informatischen Biometrie sind Handflächenabdrücke eine inzwischen auch genutzte Modalität. Ein erster Schritt bei der daktyloskopischen Untersuchung ist daher die Bestimmung der spezifischen Quelle eines Papillarleistenabdrucks.[58]

Die Automatisierung der forensischen Fingerabdruckerkennung, die ungefähr in den 1960er Jahren begann,[59] wurde zunächst an den Vorgehensweisen der Daktyloskopie orientiert:

> „Based on the observations of how human fingerprint experts perform fingerprint recognition, three major problems in designing AFISs were identified and investigated: digital fingerprint acquisition, local ridge characteristic extraction, and ridge characteristic pattern matching."[60]

---

[54] Die Begriffe *Biometrics* und *Biometrie* verwende ich synonym zu *informatische Biometrie*. Wenn ich die Biometrie im Sinne der Biostatistik meine, erwähne ich dies explizit.

[55] Hinter kursiv hervorgehobenen Begriffen werden in Klammern stets die üblichen englischen Bezeichnungen angegeben. Sollten die deutschen Begriffe im allgemeinen Sprachgebrauch unüblich sein, wird dies andersherum gehandhabt.

[56] Deutlich wird dies im *Kapitel 2.3 Allgemeine Systemarchitektur biometrischer Systeme* (S. 41) und *Kapitel 2.4 Prozesse in biometrischen Systemen* (S. 49) herausgearbeitet.

[57] Vom altgriechischen *δάκτυλος*/*daktylos* = Finger und *σκοπιά*/*skópia* = Ausschau halten, Ausspähen.

[58] Vgl. Vanderkolk 2011, S. 9-3.

[59] Vgl. Moses 2011.

[60] Maltoni u. a. 2009, S. 34.

Die Fingerabdruckabnahme erfolgte bei den Polizeien über ein Jahrhundert lang mit Tinte.[61] Bis heute wird neben den Livescan-Techniken auch massenhaft auf diese alte Methode zurückgegriffen.[62] Bei einer sogenannten *Off-line Fingerprint Acquisition* stellt die manuell erstellte Fingerabdruckkarte (siehe Abbildung 2.1) die Ersterfassung der biometrischen Charakteristik dar. Hierauf wird der mit der Tinte eingeschmierte Finger gepresst und von einer Fingernagelseite zur anderen abgerollt.

Abbildung 2.1: *Fingerprint Card* des FBI. 1. Reihe: abgerollte Einzelabdrücke rechte Hand, Daumen, Zeige-, Mittel-, Ring- und kleiner Finger, 2. Reihe: gleiche Finger linke Hand. Unten: Zur Kontrolle gleichzeitiger Gesamtabdruck von vier Fingern und Daumen linker Hand, daneben rechter Hand. Abbildung aus Cutro 2011, S. 4-5.

Latente Fingerabdrücke auf beliebigen Gegenständen werden zum Beispiel mit Rußpulvern, fluoreszierenden Pulvern und UV-Licht, Magnetpulvern, Ninhydrin oder Cyanacrylatdämpfen sichtbar gemacht und dann in der Regel hochauflösend für den späteren Vergleich fotografiert.

Für den Vergleich werden die spezifischen Merkmale eines jeden Fingerabdrucks, die für jedes Individuum einzigartig sind – so die der Praxis zwingend zugrundeliegende

[61] In der Regel handelt es sich um eine speziell für die Fingerabdruckabnahme angefertigte Tinte, die als Paste oder auf einer Art Stempelkissen erhältlich ist, vgl. coloprint GmbH 2014/2015.

[62] So ist beispielsweise beim *Federal Bureau of Investigation* (FBI) nach wie vor die Erfassung mit Fingerabdruckkarten und Tinte in den allgemeinen Verfahren für die Abnahme von Fingerabdrücken vorgesehen (vgl. CJIS o. J.). Die Anweisungen für die Abnahme von Fingerabdrücken von Asylbewerberinnen geben neben den Livescans die althergebrachte Technik vor (vgl. BAMF 2012). Die erkennungsdienstliche Behandlung in den Polizeidienststellen Deutschlands wird schon allein wegen der teuren Scanner längst nicht überall digital vorgenommen (vgl. Hahn 2015).

Annahme –,[63] genau lokalisiert und kategorisiert. Zu diesen Kategorien zählt zum Beispiel der Papillarlinienverlauf (Grundmuster oder Level-1-Typisierung), der traditionell global nach singulären Punkten, anhand eines Orientierungsfeldes der Linienrichtungen oder den räumlichen Beziehungen der Linien untereinander und lokal nach Minutien (Level-2-Typisierung) klassifiziert wird. Außerdem gehören die nur auf hoch aufgelösten Bildern erkennbaren Level-3-Merkmale wie Poren, kaum entwickelte Hautleisten oder Narben dazu. In der Abbildung 2.2 ist eine Auswahl der wichtigsten Merkmale der genannten Typen und ihrer Bezeichnungen zu sehen.

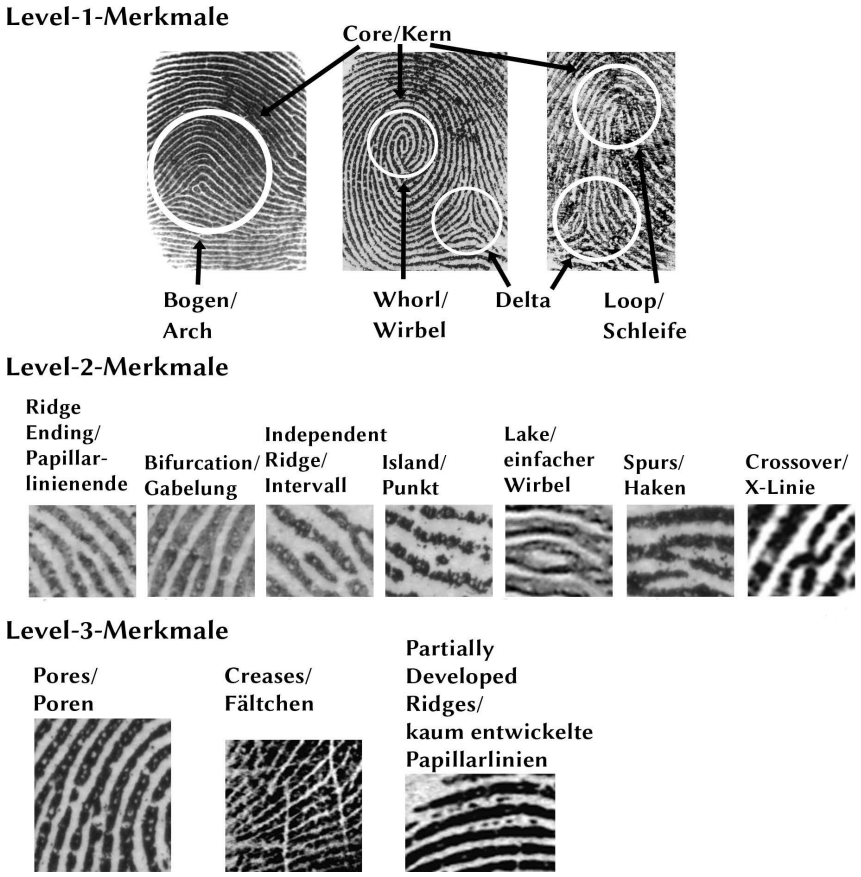


Abbildung 2.2: Beispiele für Level-1,-2,-3-Merkmale von Fingerabdruckbildern, vgl. Maltoni u. a. 2009, S. 98 ff. sowie BSI o. J. S. 5 ff.

[63] Man geht in der Kriminalistik und der Rechtsprechung bis heute davon aus, dass sich diese Annahme hinreichend bewährt hat und die empirischen und theoretischen Beweise genügen. Gleichermaßen sind die Einzigartigkeit eines jeden Fingerabdrucks und vor allem die Wissenschaftlichkeit der empirischen Nachweise in den letzten Jahrzehnten heftig umstritten gewesen – siehe hierzu vor allem Cole 2001 sowie Cole 2006. Erstere Quelle stellt insgesamt eine hervorragende kritische Geschichte der kriminalistischen Fingerabdruckerkennung dar. Mehr zum Diskurs um Eindeutigkeit im *Kapitel 4.1 Eindeutigkeit, Universalität, Permanenz als Mythos* (S. 134).

Je nach Land gibt es in der Rechtsprechung unterschiedliche Ansichten, in welcher Weise Merkmale zweier Abdrücke übereinstimmen müssen, um eine ausreichend gestützte „Identitätsvermutung“ abzugeben, also zu behaupten, dass sie von derselben Person stammen. Für Deutschland gilt beispielsweise, dass mindestens acht Minutien, wenn das Grundmuster übereinstimmt, und sonst mindestens zwölf gleich sein müssen.[64] In den USA muss ein über Jahrzehnte erarbeitetes systematisches Verfahren – *Analysis*, *Comparison*, *Evaluation* und *Verification* (ACE-V) – eingehalten werden.[65]

Es ist leicht vorstellbar, dass die Suche nach der zu einem latenten Abdruck passenden Fingerabdruckkarte in einem Archiv mit heutzutage mehreren Millionen Karten, aber auch schon mit Tausenden Karten, nur mit guten Klassifikationssystemen zu bewältigen ist. 1927 beschreibt Robert Heindl in seinem 780 Seiten umfassenden Buch »System und Praxis der Daktyloskopie und der sonstigen technischen Methoden der Kriminalpolizei« bereits mehr als 20 verschiedene polizeiliche Registriersysteme für Fingerabdruckkarten, die sich je nach Stadt unterschieden.[66] Viele von ihnen sind an den Systemen von Francis Galton, Edward Henry oder Juan Vucetich orientiert.[67] Francis Galton publizierte sein System 1892 in seinem berühmten Buch »Finger Prints«.[68] Der nach Argentinien emigrierte Kroate Juan Vucetich, anfangs Statistiker in der Zentralen Polizeidienststelle in La Plata, später Leiter der dortigen Abteilung für Anthropometrie, experimentierte aufbauend auf Galtons Arbeiten mit den Fingerabdrücken Gefangener und entwickelte ein eigenes Klassifikationssystem. Auch der britische Generalinspektor der *Bengal District Police* in Indien, Edward Henry, las Galtons Buch und die Arbeiten von Purkinje,[69] der ein anderes System entwickelt hatte. Zusammen mit seinen indischen Angestellten schuf er ein System für die Fingerabdrücke der dortigen Gefangenen,[70] das 1901 modifiziert von *Scotland Yard* übernommen wurde.

Kurz gesagt bauen alle Systeme auf Zahlen- und Buchstabenkodierungen der typisierten Hautleistenmerkmale auf den jeweiligen Fingern auf. So werden im Henry-System beispielsweise alle zehn Finger zunächst anhand des auf ihnen vorkommenden oder nicht vorkommenden Grundmusters *Whorl*, dann nach ihren Minutien und dann anhand weiterer Merkmale wie bspw. der Anzahl der Linien in den Schleifen kodiert. Schon die primäre Kodierungsstufe erlaubt hier 1024 verschiedene Einstufungen.[71]

---

[64] Vgl. Weihmann 2009, S. 63.

[65] Vgl. Ashbaugh 1999; Vanderkolk 2011; Standards der *Scientific Working Group on Friction Ridge Analysis, Study and Technology* (SWGFAST), siehe http://www.swgfast.org/, letzter Abruf: 22.7.2017.

[66] Vgl. Heindl 1927.

[67] Ein knapper Überblick zu diesen und anderen Registrierverfahren findet sich auch in Hutchins 2011.

[68] Vgl. Galton 1892.

[69] Vgl. Cummins und Kennedy 1940.

[70] Vgl. Henry 1900.

[71] Vgl. Hutchins 2011, S. 5–9.

So kann nach genauer Analyse eines latenten Abdrucks dann in einem eingegrenzten Bereich der Karteikästen nach passenden Vergleichskandidaten gesucht werden.

Wesentlich einfacher ist ein Vergleich, bei dem es beispielsweise nur um den Ausschluss oder die Bestätigung einer Übereinstimmung des Abdrucks einer schon bekannten Person mit nur einem gegebenen anderen Abdruck geht. Das ist etwa der Fall, wenn ein latenter Abdruck von einem Tatort gegen den der Person, die die Spurensicherung übernommen hat, abgeglichen wird.[72]

2.2 Grundbegriffe biometrischer Systeme

2.2.1 Biometrie und ihre Definitionen

> „Indeed, the term 'biometry' is a natural choice for anyone reaching for a way to combine measurement and biology in one name."[73]

Im »Vocabulary«-Dokument der *Working Group 1* des *Subcommittee 37 »Biometrics«* im *Joint Technical Committee* (JTC) 1 der ISO/IEC (ISO/IEC JTC 1 SC 37 WG 1) wird Biometrie als „automatisierte Erkennung von Individuen anhand ihrer verhaltensbezogenen und biologischen Charakteristika" definiert.[74]

Biometrie (*Biometrics*) wird in dieser Definition synonym mit dem Begriff *biometrische Erkennung* (*Biometric Recognition*)[75] verwendet. *Authentication* als Synonym für *Biometric Verification* oder *Biometric Identification* gelte gemäß des ISO/IEC-Vokabulars inzwischen als veraltet.[76]

Als Beispiele für verhaltensbedingte oder biologische Charakteristika, die so genannten *biometrischen Charakteristika* (*Biometric Characteristics*), auch als *Biometric Identi-*

---

[72] Ein solcher Abgleich nur zweier gegebener Abdrücke darauf, ob sie zueinander passen, wird auch in der automatisierten Fingerabdruckerkennung klar von Vergleichen eines Abdrucks mit vielen anderen, um den passenden zu finden, unterschieden. Siehe *Unterkapitel 2.2.3 Enrolment, Verifikation und Identifikation* (S. 35).

[73] Stigler 2000, S. 654.

[74] Im engl. Original: „automated recognition of individuals based on their biological and behavioural characteristics", ISO/IEC 2382-37:2017, S. 2. Die hier übernommene inoffizielle deutsche Übersetzung findet sich bei Busch o. J. Christoph Busch gehört der ISO-Arbeitsgruppe mit an. Das für 150,40 Euro zu erwerbende Dokument »DIN EN 17054 Mehrsprachiges biometrisches Vokabular, basierend auf der englischen Version der ISO/IEC 2382–37« enthält eine deutsche, englische und französische Fassung und hat bis dato den Status eines Norm-Entwurfs.

[75] Wichtige Grundbegriffe der Biometrie, die im ISO/IEC-Vokabular definiert sind, werden in den Kapiteln des Grundlagenteils bei Erstnennung kursiv gesetzt und sowohl auf Deutsch als auch Englisch angegeben. Die deutschen Übersetzungen sind in diesem Kapitel, wenn nicht anders angegeben, in der Regel derselben Quelle wie in Fußnote 74 entnommen.

[76] Vgl. ISO/IEC 2382-37:2017, S. 2, Anmerkung 6, Begriff „Biometrics".

fiers oder *Traits* bezeichnet,[77] werden „Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, handwritten signature dynamics, etc.“ angeführt.[78]

Im »Biometrics Tutorial« des Subcommittee 37 der ISO aus dem Jahre 2007 wird neben der oben genannten noch eine weitere, inzwischen beinahe 20 Jahre alte Definition angeführt, von der es heißt, sie sei weithin akzeptiert:

> „A biometric is a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity.“[79]

Obwohl es im Tutorial heißt, dass die eingangs zitierte, neuere Definition der ISO im Großen und Ganzen damit zu vereinbaren sei,[80] gibt es doch einige sehr wichtige Unterschiede. Dazu gehört der bewusste Verzicht auf den Begriff der Identität.[81] Auch Messbarkeit und Eindeutigkeit der Merkmale werden in der ISO-Definition außen vor gelassen.

Die folgende Definition ähnelt der der ISO im »Vocabulary«, aber es wird hier klarer betont, dass die genutzten Charakteristika unverwechselbare sind:

> „*Biometric recognition* (or simply *biometrics*) refers to the use of distinctive *anatomical* (e.g., fingerprints, face, iris) and *behavioral* (e.g., speech) characteristics [...] for automatically recognizing individuals.“[82]

Den bisher genannten Definitionen ist gemein, dass sie den Automatisierungsaspekt hervorheben. Im »Vocabulary« wird dies dahingehend spezifiziert, dass der Erkennungsprozess vollständig oder teilweise von einer Maschine durchgeführt wird.[83]

Eine viel kürzere Definition dagegen ist die folgende:

> „Biometrics is the identification of an individual using a distinctive aspect of their biology or behavior.“[84]

---

[77] Vgl. Maltoni u. a. 2009, S. 2.

[78] ISO/IEC 2382-37:2017, S. 2.

[79] ISO/IEC TR 24741:2007, S. 1. Die Definition stammt aus einem Text Gary Roethenbaughs von 1998, auf dem das Tutorial in einigen Teilen aufbaut (vgl. ISO/IEC TR 24741:2007, S. 57). Dieser Text ist nur noch im *Internet Archive* verfügbar: Zur Definition vgl. Roethenbaugh 1998, Section 1.

[80] Da die Verwendung von *Biometric* als Substantiv inzwischen veraltet sei (vgl. ISO/IEC 2382-37:2017, S. 1), solle dieser Begriff nur noch adjektivisch gebraucht werden (vgl. ISO/IEC TR 24741:2007, S. 1).

[81] In Unterkapitel 3.5.1 wird auf die begleitende Diskussion in der ISO-Arbeitsgruppe genauer eingegangen.

[82] Maltoni u. a. 2009, S. 2.

[83] Vgl. ISO/IEC 2382-37:2017, S. 2, Anmerkung 4, Begriff „Biometrics“.

[84] Dunstone und Yager 2009, S. 2.

Die Konkretisierung der gemessenen Charakteristika unterbleibt hier. Sie müssen lediglich eine die Individuen unterscheidende Kraft haben. Dies ist ein etwas weicheres Kriterium als Eindeutigkeit. Die folgende Definition, von der ich als Arbeitsdefinition des Begriffs *Biometrie* ausgehen möchte, macht dies noch deutlicher:

Übernommene Arbeitsdefinition des Begriffs *Biometrie*

> „Biometrik ist das automatisierte Messen eines oder mehrerer spezifischer Merkmale eines Lebewesens (e.g. einer Person). Biometrische Identifikation verfolgt das Ziel, eine mittels Biometrik spezifizierte Person von anderen unterscheidbar zu machen."[85]

Biometrik als Messvorgang an einem Lebewesen zu beschreiben behält die allgemeinere Bedeutung des Begriffs bei und erweitert sie nur um den der Automatisierung. Biometrische Identifikation ist dabei nur *ein* möglicher Prozess, in dem Biometrik zur Anwendung kommen kann. Dieser wird über sein Ziel spezifiziert, das in Bezug auf den Begriff Identifikation negativ beschrieben ist. Es geht nicht darum, die Gleichheit der Person mit sich selbst herzustellen, sondern ihre Unterscheidung von den anderen zu ermöglichen. Außerdem wird die Konstruktion des Begriffs *Person* als „eine mittels Biometrik spezifizierte" klar beschränkt.

2.2.2 Eindeutigkeit, Permanenz, Universalität, Messbarkeit, Akzeptanz

Damit ein biometrisches System überhaupt funktionieren kann, muss ein von einer biometrischen Charakteristik eines Individuums gemessenes Signal folgende Eigenschaften erfüllen:[86]

- Es muss in Bezug auf andere Individuen *unterscheidend* (*Distinctiveness*) sein. Andere Begriffe für diese Eigenschaft sind *Eindeutigkeit* (*Uniqueness*), *Between-Individual Variation* oder – werden die Signalaufnahmen ein und desselben Individuums als Teil einer Klasse von Mustern betrachtet – *Inter-Class Variation*.
- Diese Unterscheidbarkeit muss *reproduzierbar* sein. Weitere Begriffe hierfür: *Permanenz* (*Permanence*), *Wiederholbarkeit* (*Repeatability*), *Stability*.
- Jedes Individuum muss die Charakteristik besitzen, sie muss also *universal* sein. Weiterer Begriff hierfür: *Inclusiveness*.

[85] Behrens/Roth 2001, S. 10. Es handelt sich hier ebenfalls um eine vergleichsweise alte Definition, die noch vor den Debatten für das ISO/IEC-»Vocabulary« gefunden wurde, aber aus oben erläuterten Gründen präziser und treffender als die jüngeren ist.

[86] Die genannten Begriffe stammen aus ISO/IEC TR 24741:2007, S. 11, 16 f. Die ergänzten, fast synonym verwandten Begriffe sind aus Dunstone und Yager 2009, S. 12 f., 71 sowie Ross, Nandakumar und Jain 2006, S. 19.

- Außerdem muss das Signal der Charakteristik *messbar* oder *zugänglich* sein. Weitere Begriffe hierfür: *Accessibility*, *Collectability*.
- Schließlich nennen einige Autorinnen auch die Notwendigkeit der *Akzeptanz* (*Acceptability*) der Messung seitens der betroffenen Person.

Bereits bezogen auf nur ein Individuum gibt es, zum Beispiel abhängig von der Art des Auflegens eines Fingers auf einen Sensor, unterschiedlich starke Schwankungen im Grad der Ähnlichkeit verschiedener Signale derselben Charakteristik. Diese Abweichungen werden als *Intra-Class Variation* (auch: *Within-Individual Variation* oder *Non-Repeatability*) bezeichnet. Ist diese größer als die oben erwähnte *Inter-Class Variation*, wird derselbe Finger bei einer späteren Präsentation am biometrischen System als ein anderer erkannt oder als nicht zuzuordnen eingestuft.[87]

2.2.3 Enrolment, Verifikation und Identifikation

Zu typischen Anwendungsfällen der biometrischen Personenerkennung gehören etwa die Wiedererkennung autorisierter Einzelpersonen an Rechnern oder Bankkonten,[88] die Identifizierung von Straftäterinnen,[89] die De-Duplikation von Sozialleistungsempfängerinnen oder Versicherungskundinnen, die Beschränkung der Übertragbarkeit von Gruppentickets auf nicht einer Gruppe zugehöriger Personen oder die Nutzung für Watchlisten in der Einwanderungspolitik.[90]

All diese Anwendungen eint, dass die Personen, die maschinell wiedererkannt werden sollen, zunächst einmal überhaupt erfasst werden müssen. Es muss eine Referenz geben, gegen die verglichen wird. Diese wird beim sogenannten *Enrolment*, der Ersterfassung, erstellt. Die *biometrische Referenz*, die in einer *Enrolmentdatenbank* hinterlegt wird, wird aus einem bei der Vermessung erstellten *biometrischem Sample* (zum Beispiel ein JPEG-Bild) generiert. Ein Enrolment kann zu späteren Zeitpunkten wiederholt werden (*Re-Enrolment*), etwa bei Softwareanpassungen oder bei zu starker Alterung der gespeicherten Daten. Teilweise wird dem zweitgenannten Problem mit automatischer Aktualisierung der Referenz (*Biometric Reference Adaptation*) begegnet.

---

[87] Siehe auch *Unterkapitel 3.5.2*.

[88] Rechneranmeldung: Der Fingerabdruck-Sensor im IBM Thinkpad T42 (heute Lenovo) war 2004 der erste in einem mobilen Endgerät serienmäßig verbaute für den *Consumer*-Markt (vgl. Germain 2004). Banking: Diverse Banken weltweit führen immer mal wieder ein Pilotprojekt für biometriebasierten Zahlungsverkehr durch oder bieten die Möglichkeit hierfür fest an. Siehe bspw. Tassabehji und Kamala 2012 oder Gelb und Clark 2013.

[89] Die Automatisierten Fingerabdruckidentifizierungssysteme (AFIS) des FBI oder Bundeskriminalamt (BKA) sind hier Beispiele. In diesem Bereich spielt auch der Nachweis, dass die Abbilder eines biometrischen Charakteristikums nicht identifiziert oder mit einem bestimmten Abdruck in Übereinstimmung gebracht werden können, als Falsifikation einer Tatbeteiligung eine Rolle.

[90] Eurodac, Overstayer-Listen, Anti-Terror-Listen.

Laut Wayman gibt es nun zwei grundsätzliche Überprüfungen, die ein biometrisches System anhand der hinterlegten Referenzen vornehmen kann:

> „A biometric system can be designed to test one of only two possible hypotheses: (1) that the submitted samples are from an individual known to the system; or (2) that the submitted samples are from an individual not known to the system. […] This is the most important distinction between systems, and controls potential architectures, vulnerabilities and system error rates."[91]

Mit den Begriffen *biometrische Verifikation* (*Biometric Verification*) und *biometrische Identifikation* (*Biometric Identification*) werden diese beiden Fälle grob unterschieden.[92] Diese Kategorien subsumieren verschiedene Erkennungsziele.

Biometrische Verifikation wird im »Vocabulary« der ISO/IEC als „Prozess der Bestätigung einer *biometrischen Behauptung* durch einen *biometrischen Vergleich*"[93] definiert. Diese Behauptung besagt, „dass eine *zu erfassende betroffene Person* die körperliche Quelle einer bestimmten oder unbestimmten *biometrischen Referenz* ist oder nicht".[94] Im ersteren Fall ist die Rede von einer *positiven biometrischen Behauptung* (*Positive Biometric Claim*) und im letzteren von einer *negativen biometrischen Behauptung* (*Negative Biometric Claim*). Außerdem wird eine *biometrische Behauptung* auch manchmal mit *Identitätsbehauptung* (*Claim of Identity*) bezeichnet.[95] Obwohl der Begriff *Behauptung* dies zu unterstellen scheint, ist es nicht zwangsläufig so, dass die betroffene Person diese Behauptung aktiv aufstellt. Der auf diese Rolle einer betroffenen Person bezogene allgemeine Begriff lautet nichtsdestotrotz *Claimant* (*Anspruchsteller*(*-in*)).

Biometrische Identifikation wiederum ist definiert als der „Prozess der Suche in einer *biometrischen Enrolmentdatenbank*[, um] den[/die] einem einzigen Individuum zuordenbaren *biometrischen Referenzidentifikator[en]* zu finden und auszugeben".[96]

Ein typisches Beispiel für eine Verifikation ist der Abgleich eines auf einer Chipkarte hinterlegten Fingerabdrucks mit einem gerade vom Verifikationssystem erfassten. Innerhalb des Systems wird bei einer Verifikation ein *Eins-zu-Eins-Vergleich* (*One-*

---

[91] Wayman 2005, S. 5.

[92] Vgl. ISO/IEC 2382-37:2017, S. 2, Anmerkung 3, Begriff „Biometrics".

[93] Im engl. Original: „process of confirming a *biometric claim* through *biometric comparison*" (ISO/IEC 2382-37:2017, S. 19, Hervorhebung im Orig.), Übersetzung bei Busch o. J. (siehe Fußnote 74).

[94] Im engl. Original: „claim that a *biometric capture subject* is or is not the bodily source of a specified or unspecified *biometric reference*" (ISO/IEC 2382-37:2017, S. 12, Hervorhebung im Orig.), Übersetzung bei Busch o. J. (siehe Fußnote 74).

[95] Vgl. ISO/IEC 2382-37:2017, S. 12, Anmerkung 2, Begriff „Biometric Claim".

[96] Im engl. Original: „process of searching against a *biometric enrolment database* to find and return the *biometric reference identifier(s)* attributable to a single individual" (ISO/IEC 2382-37:2017, S. 18, Hervorhebung im Orig.), Übersetzung bei Busch o. J. (siehe Fußnote 74).

to-One Comparison) der biometrischen Probe einer betroffenen Person mit der biometrischen Referenz einer betroffenen Person vorgenommen.

Im Unterschied dazu erfordert eine Identifikation einen *Eins-zu-N-Vergleich* (*One-to-Many Comparison*). Dies ist der Fall in den AFIS der Polizeien. Im Falle einer Identifikation wird die *biometrische Referenzdatenbank* (*Biometric Reference Database*) des Systems durchsucht (*Biometric Search*), um herauszufinden, ob die Referenz in der Datenbank enthalten ist. Es kann auch eine Liste möglicherweise passender Referenzen gefunden werden, die *biometrische Kandidatenliste* (*Biometric Candidate List*). Neben der Information, dass die betroffene Person schon einmal in der Datenbank erfasst worden ist, können auch weitere beim Enrolment hinterlegte Daten wie Name oder Geburtsdatum in der Enrolmentdatenbank gespeichert sein.

Verifikation und Identifikation schließen sich nicht gegenseitig aus. Manchmal wird die Verifikation bezogen auf die Anzahl der Mustervergleiche auch als Spezialfall der Identifikation gesehen, da nur zwei Muster verglichen werden und N=1 ist.[97] Andererseits kann die Identifikation auch als eine Abfolge von N 1-zu-1-Vergleichen gesehen werden.[98] Auch die Identifikation beinhaltet eine zu verifizierende Behauptung, nämlich dass jemandes biometrische Daten in einer Datenbank hinterlegt sind oder nicht.[99]

Wie die beiden Anwendungsarten in die Funktionsweise des Systems eingebettet sind, wird in den folgenden beiden Kapiteln genauer erläutert.

2.2.4 Rollen der Interaktion von Mensch und Biometrie-System

Der Mensch, um dessen Erkennung es in der informatischen Biometrie geht, wird zum ihn messenden System sehr verschieden ins Verhältnis gesetzt. Einige hierfür oft genutzte Begriffe sollen kurz vorgestellt werden. In den oben angeführten Biometrie-Definitionen ist von *Individuen*, *Lebewesen* oder aber *Personen* die Rede, deren Identifizierung oder Unterscheidung ermöglicht werden soll. Im Biometrie-Vokabular der ISO/IEC wird absichtlich auf den Begriff der Person verzichtet, da biometrische Technologien Personen individualisieren und es um natürliche statt um juristische Personen geht.[100] Für die Zukunft prognostiziert die Autorengruppe des »Vocabulary« zudem eine Ausweitung der Biometrie auf die Verarbeitung von DNA, die die individuumbezogene Definition der Biometrie ändern würde. Denn dann sei auch die Erkennung genetischer Beziehungen zwischen Individuen und ihre Erkennung anhand von Samples anderer Individuen oder Gruppen von Individuen möglich.[101]

---

[97] Wayman, Jain u. a. 2005, S. 6 f.: „Identification systems are said to compare samples from one person to templates from many persons, with verification being the degenerate case of 'many' equal to one."

[98] Vgl. Maltoni u. a. 2009, S. 15.

[99] Vgl. Wayman, McIver u. a. 2014, S. 7.

[100] Vgl. ebd., S. 4.

[101] Vgl. ebd., S. 7.

Der Oberbegriff für alle mit einem biometrischen System interagierenden Personen oder Organisationen ist der *User*. *End User* ist dagegen laut »Vocabulary« nicht mehr gebräuchlich. Der User, dessen Daten erfasst und verglichen werden, wird als *Biometric Capture Subject* oder *Biometric Data Subject*/*Biometric Enrolee* bezeichnet, jeweils in Abhängigkeit davon, ob die biometrischen Charakteristika noch erfasst werden bzw. schon erfasst und im System hinterlegt sind. Die deutsche Übersetzung dieser Termini lautet „zu erfassende betroffene Person" bzw. „betroffene Person"[102] und orientiert sich damit an den Sprachgepflogenheiten juristischer Datenschutzregelungen im Englischen und Deutschen.[103]

Die Begriffe *Biometric System Operator* oder *Biometric Attendant* (*biometrischer Betreuer*) beschreiben Funktionen des Betriebspersonals, die auch User sind. Ersterer ist für die Administration und Implementation bestimmter Verhaltens-, Wartungs- und Konfigurationsregeln (*Policies*) im Umgang mit einem biometrischen System verantwortlich, letzterer unterstützt die betroffene Person beim Enrolment-Prozess oder späteren Akquisitionsprozessen. Die komplette Verantwortung trägt im Idealfall die Systemeigentümerin (*Biometric System Owner*), die eine Person oder eine Organisation sein kann.

User werden zusätzlich anhand ihres Kooperationsverhaltens genauer eingeteilt: Ein *subversiver User* (*Subversive Biometric Capture Subject*, *Subversive User*) versucht die für ein biometrisches System vorgesehenen Regeln zu umgehen. Speziell wird von einem *Impostor* (in der inoffiziellen deutschen Variante des genormten biometrischen Vokabulars mit *nichtauthentische Person* übersetzt) gesprochen, wenn eine zu erfassende betroffene Person „versucht[,] mit der biometrischen Referenz einer anderen Person Übereinstimmung zu erlangen".[104] Von einem *Verdecker einer Identität* (*Identity Concealer*) ist die Rede, wenn eine zu erfassende betroffene Person „versucht[,] sich einer Übereinstimmungsentscheidung mit der eigenen biometrischen Referenz zu entziehen".[105] *Nicht-subversiv* oder *kooperativ* sind natürlich auch mögliche Verhaltensklassifikationen. Neben den betroffenen Personen gelten beispielsweise auch Administratorinnen, die unberechtigte Personen zulassen oder bestimmte Datenschutzregeln nicht einhalten, als subversive Benutzerinnen.

Der Begriff (*Non-*)*Conformant Capture Attempt* ((*nicht-*)*konformer Erfassungsversuch*) beschreibt eine (nicht) anforderungsgerechte Präsentation, die mit entsprechend trai-

[102] Die deutsche Übersetzung findet sich bei Busch o. J.

[103] So wird im Kontext der Definition der Begriffe *Personal Data* (*personenbezogene Daten*) in 95/46/EC Art 2[a] sowie EU-GDPR Art 4(1) „data subject" als Bezeichnung für „an identified or identifiable natural person" verwendet und im deutschen Pendant, Artikel 2 Buchstabe a 95/46/EG sowie Artikel 4 Absatz 1 EU-DSGVO, also an gleicher Stelle, „betroffene Person" für „eine bestimmte oder bestimmbare natürliche Person" bzw. „eine identifizierte oder identifizierbare natürliche Person".

[104] Busch o. J.

[105] Ebd.

nierten oder absichtlichen Verhaltensweisen betroffener Personen zu tun haben kann, aber nicht muss. So kann eine *kooperative Präsentation* bei schlechtem Training auch unpassend und damit erfolglos bleiben, genauso wie eine *unkooperative Präsentation* (*Uncooperative Presentation*) durchaus auch zu einem in dem Falle wohl eher unerwünschten passenden Erfassungsversuch führen kann. In Fällen erkennungsdienstlicher Behandlung kommt es vor, dass das polizeiliche Personal die Kooperation mit Gewalt erzwingt. Auch die gleichgültige Art der Präsentation, bei der die betroffene Person weder kooperativ noch unkooperativ ist, wird klassifiziert. Sie wird als *Indifferent Presentation* bezeichnet und ist auf Deutsch einmal mit „unbekümmert" und ein anderes Mal mit „nicht bewusst" eher unpassend übersetzt.[106]

Eine weitere im ISO/IEC-Vokabular erwähnte Rolle ist die des *Biometric Characteristics Examiner*, wie es beispielsweise eine Daktyloskopin wäre. Sie prüft biometrische Charakteristika und die Korrektheit des Vergleichs manuell. Diese Rolle impliziert einen behördlich autorisierten Expertinnenstatus.

Schließlich spielen personenbezogenene Termini eine wichtige Rolle in der Klassifizierung biometrischer Systeme je nach Anwendungskontext. Dieser beeinflusst maßgeblich die verschiedenen Rollen, die die betroffenen Personen spielen können oder zu spielen gezwungen sind. Taxonomien für die verschiedenen Anwendungskontexte werden in Kapitel 3.1 vorgestellt.

2.2.5 Datenkonzepte

Je nach Verarbeitungsstufe werden die in einem Biometrie-System prozessierten Daten unterschiedlich bezeichnet. Insgesamt werden sie als analoge oder digitale Repräsentationen biometrischer Charakteristiken unter dem Oberbegriff *biometrische Daten* (*Biometric Data*) zusammengefasst.[107] Unter ihn fallen nicht nur die erfassten und verarbeiteten Bilddaten, sondern auch universelle Modelle biometrischer Daten, wie sie etwa in trainierten Klassifikatoren genutzt werden,[108] oder bestimmte *biometrische Eigenschaften* (*Biometric Properties*). Diese sind Beschreibungen einer betroffenen Person, die automatisch aus dem Sample gewonnen/geschätzt werden können. Dazu gehören beispielsweise bei Fingerabdrücken die Klassifizierung des Papillarleistenverlaufs oder bei der Gesichtserkennung Attribute wie Alter oder Geschlecht. Bezogen auf die Bilddaten werden diese Repräsentationen *vor* der Merkmalsextraktion *Biometric Samples* genannt, auch wenn sie möglicherweise schon eine gewisse Bildverarbeitung wie

[106] Ebd. Der Begriff „indifferent biometric capture subject" wird in ISO/IEC 2382-37:2017, S. 17 definiert als „*biometric capture subject* who is unconcerned with the achievement of a successful *biometric acquisition process*"; „indifferent presentation" als „presentation in which the *biometric capture subject* is unconcerned that the *biometric capture process* is occurring" (ISO/IEC 2382-37:2017, S. 13).

[107] Die im Folgenden aufgelisteten Termini und ihre Definitionen orientieren sich auch hier an ISO/IEC 2382-37:2017, S. 3 ff.

[108] Siehe *Unterkapitel 2.4.4 Biometrie und Maschinenlernen* (S. 66).

Kontrastverstärkung oder Kompression durchlaufen haben – ein JPEG 2000-Bild eines Fingerabdrucks ist ein Beispiel hierfür. Ein Sample kann auch analog sein – eine Fingerabdruckkarte ist ebenfalls ein Sample.[109] Ein weiterer Verarbeitungszustand biometrischer Daten sind dann die *Biometric Features* (*biometrische Merkmale*). Der Begriff *Merkmal* ist eigentlich irreführend, denn es handelt sich oft nicht um an der biometrischen Charakteristik selbst unmittelbar nachvollziehbare anthropometrische Maße wie im Falle einer Gesichtserkennung etwa Lippenbreite, Augenabstand, Nasenlänge oder ähnliches.[110] Die numerischen Werte, die die Features bilden, sind abstraktere mathematische Repräsentationen solcher Eigenschaften.

Werden diese formalisierten biometrischen Merkmale als Referenzen für einen späteren Vergleich abgespeichert, nennt man sie *biometrische Templates* (*Biometric Templates*) oder synonym hierzu *Referenz-Merkmalsvektoren* (*Reference Biometric Feature Set*). Nicht immer sind die erfassten Merkmalsdaten als Menge aus numerischen Informationen oder Kurzbezeichnern in Vektoren gespeichert, sondern in einigen Fällen werden andere mathematische Funktionen gewählt, wie sie beispielsweise das Hidden-Markov-Model, Gauß-Mischverteilungen oder Künstliche Neuronale Netzwerke nutzen. In diesem Fall ist die Rede von *biometrischen Modellen* (*Biometric Models*). In Verbindung mit einer Zuordnung zu einer betroffenen Person werden hinterlegte Samples, Templates oder Modelle allgemein auch als *biometrische Referenzen* (*Biometric References*) bezeichnet. Der Begriff „Referenz“ verdeutlicht, dass diese Daten einen eindeutigen Zeiger auf einen durch das System erfassten Menschen darstellen. Es gibt verschiedene Arten der Verknüpfung von Personendaten mit biometrischen Referenzen. Hierzu können sowohl biographische Daten wie Name und Geburtsdatum o. ä. als auch „weiche“ oder demographische biometrische Daten gehören.[111] Biometrische Daten, die zur Generierung sogenannter Hintergründe genutzt werden, wie sie in bestimmten Verfahren der Mustererkennung gebräuchlich sind, um typische Eigenschaften von Fingern, Gesichtern, Stimmen o. ä. formal zu generieren, sind keine Referenzen.

Wird ein biometrisches Sample oder ein biometrisches Merkmal als Eingabe für den Vergleich mit einer gespeicherten biometrischen Referenz genutzt, wird dieser Vorgang bzw. dieses Merkmal als Eingabedatum auch *biometrische Abfrage* (*Biometric Probe*/synonym: *Biometric Query*) genannt.[112]

---

[109] Siehe Abbildung 2.1.

[110] Vgl. ISO/IEC TR 24741:2007, S. 11.

[111] In Jain, Flynn und Ross 2008a, S. 5 bspw. werden zusätzlich in einer Biometrie-Datenbank hinterlegte Daten wie Körpergröße, Augenfarbe, Geschlecht (*Gender*) oder Ethnizität als *Soft Biometrics* bezeichnet. Bei Maltoni et al. 2009 ist von „demographic information“ die Rede (Maltoni u. a. 2009, S. 5).

[112] In der inoffiziellen deutschen Übersetzung des ISO/IEC-Vokabulars (siehe Fußnote 74) wird *probe* mit *Probe* übersetzt, die sich in Bezug auf das Datum selbst zwar gut eignet, aber ungewöhnlich ist. Die Begriffe *biometrischer Testdatensatz* oder in Bezug auf den Vorgang *Untersuchung* oder *Test* wären hier eine geeignetere Übersetzung.

In Bezug auf die Speicherung dieser Daten in verschiedenen Datenbankmanagementsystemen wird nochmals terminologisch differenziert in:

- *biometrischer Datensatz* (*Biometric Data Record*), der biometrische und nichtbiometrische Daten (wie eben Name, Alter o. ä.) enthalten kann,
- *biometrischer Referenzdatensatz* (*Biometric Reference Data Record*), der als indizierter Datensatz biometrische Referenzen enthält,
- *Identifikator einer biometrischen Referenz* (*Biometric Reference Identifier*), der als Zeiger auf einen biometrischen Referenzdatensatz dient,
- *biometrischer Enrolmentdatensatz* (*Biometric Enrolment Data Record*), der nichtbiometrische Daten einer betroffenen Person und einen oder mehrere Identifikatoren von einer oder mehreren zu dieser Person gehörigen biometrischen Referenz(-en) enthält.

2.3 Allgemeine Systemarchitektur biometrischer Systeme

Fingerbilderkennungssysteme sind konkrete Anwendungsfälle digitaler signal- oder spezieller bildverarbeitender und mustererkennender Systeme.[113] Die durch das biometrische Merkmal spezifisch veränderten und mit einem Sensor gemessenen physikalischen Größen (bspw. Schall, elektrisches Feld, optische Strahlung) stellen Signale dar. Aus Sicht der Signalverarbeitung sind Signale sich zeitlich oder räumlich verändernde physikalische Größen, deren Parameter Informationen über den Zustand des betrachteten physikalischen Systems enthalten können.[114]

Nach Massen oder Jähne lassen sich die Komponenten bildverarbeitender Systeme orientiert am „visuellen System des Menschen und der Tierwelt“[115] in die drei Teile *Sehen*, *Erkennen*, *Entscheiden* gliedern.

In der Bildverarbeitung geht es vornehmlich um die Reduktion der Bilddaten auf für deren Klassifizierung relevante Informationen – hier liegt auch der Fokus der Mustererkennung (*Pattern Recognition*, *Pattern Classification*).

---

[113] Vgl. ebd., S. xii. Mustererkennung wird auch häufig als Teil der Digitalen Bildverarbeitung betrachtet (vgl. Gonzalez und Woods 2007, S. 24 f.) und erweitert diesen Bereich durch die Fähigkeiten zu Analyse und Klassifikation zum sogenannten Maschinensehen (vgl. Rosenfeld und Wechsler 2000, S. 101).

[114] Vgl. Meffert und Hochmuth 2004, S. 14.

[115] Massen 1996, S. 2. Jähne weist in seinem Grundlagenwerk zu digitaler Bildverarbeitung darauf hin, dass „[m]aschinelle Bildverarbeitung […] ohne das *menschliche Sehsystem* undenkbar“ sei. „Jedes Bild, ob direkt aufgenommen oder von einem Rechner verarbeitet, können wir nur mit Hilfe unseres visuellen Systems beurteilen“ (Hervorhebung im Orig., Jähne 2012, S. 17). De facto geht es bei der Entwicklung des maschinellen Sehens auch um die Schaffung eines „universellen maschinellen Bildverarbeitungssystem[s][…], das Bilder ‚versteht‘, wie Menschen es können“ – ein Szenario, das Jähne für eine ferne Zukunft prognostiziert (ebd., S. 19).

Die zentralen Aufgaben der Mustererkennung sind das Erkennen eines Objektes, das als solches vorher schon einmal gesehen wurde, sowie das Kategorisieren eines Objekts mit neuer Form, das vorher noch nicht gesehen wurde. Die Begriffe Kategorisieren und Erkennen sind hierbei auswechselbare Begriffe, denn sie betreffen das Klassifizieren oder Identifizieren von Mustern.[116] Im Rahmen der Mustererkennung wird das Klassifizierungsproblem statistisch gefasst:

> „The pattern recognition problem is a particular case of the more general problem of statistical regression; it seeks an approximating function that minimizes the probability of misclassification error."[117]

Um Objekte zu erkennen, werden Hypothesen über deren mathematische Klassifizierung aufgestellt, sensorisch aufgezeichnete Daten verarbeitet, aus denen das Rauschen gefiltert wird, und die am besten passenden mathematischen Modelle für die erkannten Muster gewählt.[118] Die Grundfrage ist also: Mittels welcher Gleichungen (Funktionen, Modelle) kann ich aus gesammelten, zählbaren Daten kategorisierbare Muster- oder Objektbeschreibungen gewinnen, mit denen es möglich ist, andere Objekte verlässlich dazu in Beziehung zu setzen, also zum Beispiel diese dem bereits beschriebenen Objekt als ähnlich oder verschieden zu klassifizieren?

In den grundlegenden Werken des Fachgebiets wird häufig kurz konstatiert, dass die Fähigkeit Muster zu erkennen, ein zentrales Merkmal von Intelligenz[119] und entscheidend für menschliches Überleben sei.[120] Erkenntnistheoretische Fragen wie etwa die, ob Objekte anhand der Ähnlichkeit zu bestimmten Beispielen oder anhand prototypischer Vorgaben erkannt werden, werden schnell entschieden und dann modelliert.

Ein biometrisches System besteht im Allgemeinen aus den folgenden Teilsystemen (auch: Komponenten, Modulen, Subsystemen, Operations- oder Funktionseinheiten):

- *Datenerfassungsteilsystem* (*Biometric Capture Subsystem*),
- *Signalverarbeitungsteilsystem* (*Signal Processing Subsystem*),
- *Vergleichsteilsystem* (*Comparison Subsystem*),
- *Entscheidungsteilsystem* (*Decision Subsystem*),

[116] Vgl. Rosenfeld und Wechsler 2000, S. 102; auch im Standardwerk zur Mustererkennung von Duda, Hart, Stork werden die Begriffe synonym verwendet, vgl. Duda, Hart und Stork 2001, S. 13.

[117] Rosenfeld und Wechsler 2000, S. 101.

[118] „The overarching goal and approach in pattern classification is to hypothesize the class of these models [descriptions of specified objects in a mathematical form, Anm. d. Verfasserin], process the sensed data to eliminate noise (not due to the models), and for any sensed pattern choose the model that corresponds best." (Duda, Hart und Stork 2001, S. 2).

[119] Vgl. Rosenfeld und Wechsler 2000, S. 101.

[120] Vgl. Duda, Hart und Stork 2001, S. 1.

- *Datenübertragungsteilsystem* (*Transmission Subsystem*),
- *Teilsystem zur Datenspeicherung* (*Data Storage Subsystem*),
- *Administrationsteilsystem* (*Administration Subsystem*) und
- *Technische Schnittstellen* (*Interfaces*).[121]

Diese konzeptuellen Komponenten können hochintegriert als *System-on-a-Chip*, *System-on-Card* oder *System-on-Device* komplett auf einem Chip, einer Smartcard oder in einem Scannergerät als Schaltkreis zusammengestellt sein oder auch als einzelne physische Komponenten bzw. separate Programmpakete fungieren, die in verschiedenen Systemen verbaut sind. Eine geschlossene Integration vieler Komponenten wird insbesondere in Hinblick auf *Verschlüsselungs- und Datensicherheitsmechanismen* vorgenommen. Auch wenn diese in der Regel nicht als eigene Komponente in den Darstellungen generischer Systeme aufgeführt, sondern oft gesondert betrachtet werden, haben sie erheblichen Einfluss auf die Systemarchitektur. Die Hard- und Software-Module können zudem nicht nur räumlich integriert, sondern auch zeitlich parallelisiert sein. So kann beispielsweise die Bildanalyse schon während der Sample-Akquise einsetzen und diese unmittelbar optimieren.[122]

Abbildung 2.3 zeigt die ersten sechs der oben genannten typischen Bestandteile eines Fingerabdruckerkennungssystems. Sie ist nur eine von vielen möglichen schematischen Darstellungen eines biometrischen Systems, die zentrale Elemente der Bildverarbeitung und Mustererkennung integriert.[123] Während *Transmission Subsystem* und *Interfaces* hier nicht explizit visualisiert sind, wurde die *Performance Evaluation* als konzeptuelle Komponente in die Abbildung eingefügt, da sie eine große Bedeutung für die Abstimmung einzelner Parameter sämtlicher zuvor benannter Bausteine des laufenden Systems und einen zwar nicht unbedingt automatisierten, sondern über nachträgliche Konfigurationsanpassungen menschlich vermittelten Einfluss auf ein System hat.[124] In Verbindung mit einer *Knowledge Base* lässt sich hier allerdings ein gewisser

[121] Diese Aufteilung entspricht der des *Subcommittee 37 »Biometrics«* des JTC 1 von ISO/IEC, vgl. ISO/IEC TR 24741:2007, S. 9 ff. Siehe auch *Unterkapitel 2.4.5 Technische Schnittstellen eines Biometrie-Systems* (S. 68) sowie *Abschnitt: Standardisierte Speicher- und Austauschformate* (S. 70).

[122] Vgl. Setlak 2009, S. 96.

[123] In *Kapitel 4.2 Unterschiede in der Beschreibung der Systemarchitektur* (S. 144) werden andere schematische Darstellungen beispielhaft hinsichtlich ihrer verschiedenen Schwerpunkte, die sie durch die bildliche Darstellung legen, analysiert.

[124] Rosenfeld und Wechsler sehen die *Performance Evaluation* daher als vierte Komponente eines Mustererkennungssystems. Dessen andere Komponenten sind: 1. Datenakquise/Datensammlung, 2. Feature-Extraktion und -Repräsentation, 3. Ähnlichkeitserkennung und Musterklassifikatordesign, vgl. Rosenfeld und Wechsler 2000, S. 101.

Automatisierungsgrad bis hin zur Anwendung von Methoden des maschinellen Lernens erreichen.[125]

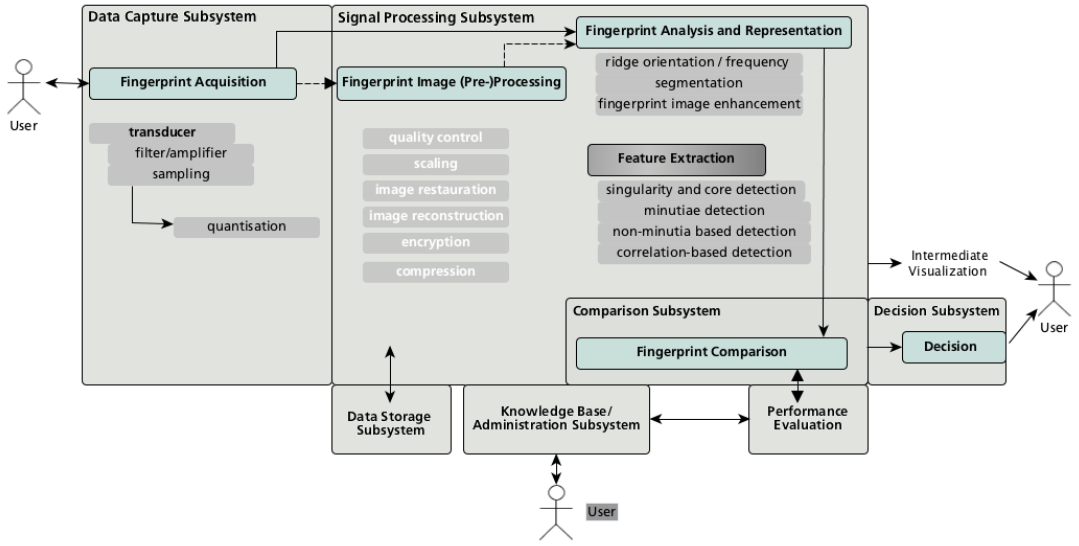


Abbildung 2.3: Bildverarbeitungskomponenten eines Fingerabdruckerkennungssystems. Eigene Darstellung.

Im Folgenden werden die einzelnen Komponenten überblicksartig hinsichtlich ihrer funktionalen Bedeutung im Gesamtsystem erläutert. Auf einzelne Teilprozesse wird im *Kapitel 2.4 Prozesse in biometrischen Systemen* (S. 49) genauer eingegangen.

Datenerfassungsteilsystem

Hierzu gehören die Präsentation eines biometrischen Charakteristikums, die einen menschlichen Akteur involviert, sowie die Sensortechnik selbst. Die *Signalerfassung* (*Signal Acquisition*), in diesem Falle die *Fingerprint Acquisition*, des für die digitale Bildverarbeitung bestimmten Signals erfolgt mittels von den Messfühlern/Sensoren (*Transducer*) aufgezeichneten Spannungs-, Ladungs-, Schall- oder Lichtintensitätsunterschieden (siehe *Unterkapitel 2.4.1 Datenerfassung und Sensortechnik* (S. 49)). Die mikrometergroßen Sensorplättchen, die meist als Matrix auf einer Sensorplatte angeordnet sind, müssen Pixelrasterweiten aufweisen, die eine verlustfreie Abtastung (*Sampling*) der Fingeroberfläche in Bezug auf den Vergleichszweck ermöglichen. Das bedeutet, dass Größe, Anordnung und Anzahl der Sensorplättchen in Bezug auf die Nyquistfre-

[125] Gonzalez und Woods sehen die *Knowledge Base* sowohl als Datenbasis für die problembezogene Logik des Bildverarbeitungssystems als auch als allgemeines Administrationsteilsystem, das die Interaktion zwischen den Modulen steuert, vgl. Gonzalez und Woods 2007.

quenz[126] eines durchschnittlichen Fingerbildes so konstruiert sein müssen, dass kein Alias-Effekt durch eine Nichteinhaltung des Abtasttheorems zustandekommt,[127] also evtl. Muster im digitalisierten Signal erzeugt werden, die im Original nicht enthalten sind. In diesem Sinne übernehmen die Sensoren hier die Bandbegrenzungsfunktion wie ein Tiefpassfilter (*Filter/Amplifier*). Außerdem werden gegebenenfalls direkt hinter die Sensorik Signalverstärker geschaltet.[128]

Die nun ortsdiskreten Signale, in zweidimensionalen Bildpunktfeldern mit festen Abständen angeordnet, werden bei der Quantisierung (*Quantisation*) Zahlwerten zugeordnet. Im konkreten Fall wird die „gemessene Bestrahlungsstärke" in Form sogenannter Intensitätswerte „auf eine begrenzte Anzahl […] diskreter Grauwerte abgebildet".[129]

Signalverarbeitungsteilsystem

Nun beginnt die *Signalverarbeitung* (*Signal Processing*), spezifisch das *Fingerprint Image (Pre-)Processing*. In einer ersten Vorverarbeitung können bestimmte Qualitätsprüfungen, Bildzerlegungen oder -zusammensetzungen (je nach verwendeten Sensoren), Skalierung oder Bildrestaurierungsverfahren zur Anwendung kommen. Außerdem werden die Bilder für ihre längerfristige Speicherung und für die Datenübertragung in der Regel komprimiert (siehe *Abschnitt: Bildformate und Speichertechniken* (S. 55)), seltener auch verschlüsselt. Die *Fingerbildanalyse und -repräsentation* (*Fingerprint Analysis and Representation*) ist dann die Prozesskomponente, in der die anwendungsrelevanten Merkmale des Bildes extrahiert werden. Auch allgemein in der Bildverarbeitung verbreitete Verfahren wie die Segmentierung zur Freistellung des eigentlich merkmalstragenden Anteils des Bildes, verschiedene übliche Bildverbesserungstechniken (*Fingerprint Image Enhancement*) beispielsweise aus den Bereichen der Punktoperationen wie Kontrast-, Helligkeitsfilter oder Nachbarschaftsoperationen (Faltungsfilter) sind Teil der Bildanalyse, die der korrekten Auffindung aller vergleichsrelevanten Merkmale für die *Merkmalsextraktion* (*Feature Extraction*) dienen. Eine besondere Rolle spielt hier die Qualitätskontrolle. Unzulängliche Qualität extrahierter Features kann zu einer Neuanforderung der Datenerfassung führen oder zur Beeinflussung der Folgeprozesse derart, dass das Template des „poor quality input sample" höheren Anforderungen beim

[126] Die Nyquistfrequenz f_N entspricht der halben Abtastfrequenz. Der Frequenzbereich des Signals darf $-f_N$ nicht unter- und f_N überschreiten, vgl. Meffert und Hochmuth 2004, S. 27.

[127] Ebd. Nach dem Nyquist-Shannon-Abtasttheorem ist ein zeit- oder ortsdiskret abgetastetes Signal nur dann verlustfrei rekonstruierbar, wenn es mit einer doppelt so hohen Frequenz abgetastet wird wie die höchste für die Nutzung relevante Frequenz, die im Signal selbst enthalten ist (vgl. ebd., 24ff.).

[128] Setlak beschreibt dies beispielsweise für Radiofrequenz-Fingerbildsensoren (vgl. Setlak 2004, S. 39).

[129] Jähne 2012, S. 165.

Vergleich genügen muss.[130] Die verschiedenen Verfahren werden genauer unter *Unterkapitel 2.4.2 Fingerbildverarbeitung und Merkmalsextraktion* (S. 56) besprochen.

Vergleichsteilsystem

Mittels des *Vergleichsteilsystems* werden gespeicherte mit gerade erst gewonnenen Merkmalen verglichen (*Fingerprint Comparison* – siehe *Unterkapitel 2.4.3 Ähnlichkeitserkennung und Musterklassifikatordesign* (S. 64)) und ein *Vergleichswert* (*Comparison Score*) berechnet. Dieser ersetzt gemäß »Vocabulary« von ISO/IEC den veralteten Begriff *Matching Score* oder *Match Score*. Der im »Biometrics Tutorial« noch verwendete Begriff *Similarity Score* ist im »Vocabulary« ein Unterbegriff des Vergleichswerts, wie auch *Dissimiliarity Score*. Ersterer steigt, letzterer verringert sich mit zunehmender Ähnlichkeit biometrischer Merkmale und wird auch *Distance Score* (*Abstandswert*) genannt. Diese Werte sind entscheidend für die Berechnung der Systemfehler, wie in *Unterkapitel 3.2.2 Systemfehler und Performanzmetrik* (S. 95) ausgeführt wird.

Entscheidungsteilsystem

Im *Entscheidungsteilsystem* wird schließlich geprüft, ob der Vergleichswert eine bestimmte Schwelle über- oder unterschreitet und je nachdem das Resultat als hinreichende Ähnlichkeit zweier verglichener Muster interpretiert werden kann oder eben nicht. Die Höhe des *Schwellwerts* (*Threshold*) – entweder fest gesetzt oder Ergebnis des Vergleichs verschiedener Kandidaten –[131] sowie die Wertung der Entscheidung als positives oder negatives Verifikations- oder Identifikationsergebnis können administrativ über *Entscheidungsrichtlinien* beeinflusst werden. Das bedeutet auch, dass die Deutung des gesamten Mustererkennungs- und Vergleichsprozesses als Verifikation oder Identifikation erst in diesem letzten Modul stattfindet. Eine steigende Anzahl mit einem einzigen Testdatensatz verglichener biometrischer Referenzen wirkt sich allerdings auf alle anderen Teilkomponenten ebenfalls aus, da sie eine andere Datenzugriffsstruktur erfordert, einen erhöhten Datendurchsatz und höhere Anforderungen an Extraktions- und Vergleichsgenauigkeit und damit Merkmalsqualität mit sich bringt.

Die auf den erzeugten Vergleichswerten beruhende *Entscheidung* (*Decision*) über die Ähnlichkeit zweier Bilder ist schließlich die Ergebnisausgabe des Gesamtsystems. Neben dieser Ausgabe kann allerdings zu jedem Zeitpunkt des Prozesses eine zusätzliche *Visualisierung* (*Intermediate Visualization*) erfolgen, die noch weitere Signalverarbeitungsstufen beispielsweise zur Rekonstruktion eines für die Nutzerin verständlichen Bildes notwendig machen.

---

[130] ISO/IEC TR 24741:2007, S. 11.

[131] „The decision can be based on a preset threshold or comparative result." (Du 2013, S. 6).

Datenübertragungsteilsystem

Für das Teilsystem der *Datenübertragung* müssen klassische nachrichtentechnische Probleme zur Informationserhaltung bei Übermittlung der Daten über einen Kanal, Probleme der Kompression und Dekompression sowie der Ent- und Verschlüsselung der Daten behandelt werden. Ob die Kompression vor der Signalverarbeitung stattfindet, die Daten bereits direkt nach der Erfassung schon lokal prozessiert, erst danach gepackt und/oder verschlüsselt zu einem räumlich entfernten Speicher übermittelt und so abgelegt werden oder ob sie sogar nach der Merkmalsextraktion noch gepackt bleiben, ist von System zu System unterschiedlich. Es ist sogar in einigen Anwendungen möglich, dass durch bestimmte Formen der Kompression der Mustervergleich erleichtert wird. Im Allgemeinen aber führt Kompression von Daten zu Qualitätsverlust im aufgenommenen Signal.[132]

Teilsystem zur Datenspeicherung

Das Subsystem zur *Datenspeicherung* ist meist ein zentrales oder verteiltes Datenbanksystem, aber es ist auch möglich, dass es nur der Speicher auf einer Chipkarte mit einem einzigen gespeicherten Fingerabdruck ist. Eine Speicherung im Erfassungsmodul, auf einem lokalen Server oder Personalcomputer ist ebenfalls möglich. In Szenarien, in denen 1-zu-N-Vergleiche nötig sind, wird allerdings eine zentralisierte oder verteilte, evtl. aber nach Alter, Geschlecht oder aus den Merkmalen selbst abgeleiteten Klassifikatoren partitionierte Architektur gewählt, bei der alle bzw. auf jeden Fall mehrere gespeicherte(n) Daten verglichen werden können. Allerdings wird auch bei sogenannten 1-zu-1-Systemen, die über eine eindeutige Referenz auf nur einen zu vergleichenden Datensatz zurückgreifen – beispielsweise, wenn es nur den einen auf der Chipkarte gespeicherten gäbe –, häufig eine zentralisierte oder verteilte Struktur verwendet. Als Gründe hierfür werden die Möglichkeit zur Neuausstellung verlorener Karten oder die Verhinderung der Erstellung gefälschter Karten angegeben.[133]

Um beispielsweise Sicherheit, Datenschutz oder Antwortzeiten zu verbessern, ist die *biometrische Referenzdatenbank* (*Biometric Reference Database*) nicht unbedingt Teil der Enrolmentdatenbank. Dann besteht die Verknüpfung zu den indizierten biometrischen Referenzdatensätzen nur noch mittels der in der Enrolmentdatenbank abgelegten Identifikatoren einer biometrischen Referenz. Ist zu einer *Enrollee* kein biometrisches Datum abgelegt, ist die assoziierte Referenz leer (NULL). Einer betroffenen Person können durchaus verschiedene Referenzdaten oder aber ein Datensatz kann mehrfachem Enrolment einer Person zugeordnet sein.

---

[132] Vgl. ISO/IEC TR 24741:2007, S. 10.

[133] Vgl. ISO/IEC TR 24741:2007, S. 12.

Administrationsteilsystem

In diesem Subsystem wird „die gesamte Reglementierung, Implementierung und Nutzung eines biometrischen System in Übereinstimmung mit den relevanten gesetzlichen und gesellschaftlichen Bedingungen und Anforderungen“ bestimmt.[134] Hierzu werden im »Biometrics Tutorial« folgende Teilaspekte aufgezählt:[135]

- Feedback an die betroffene Person vor und nach der Datenerfassung,
- Anfordern zusätzlicher Informationen von der betroffenen Person,
- Speichern und Formatieren der biometrischen Referenzen oder der Austauschdaten,
- finale Entscheidung zur Ausgabe des Entscheidungsmoduls bzw. den Vergleichswerten,
- Festlegen der Schwellwerte,
- Festlegen der Einstellungen für die biometrische Erfassung,
- Kontrolle des operativen Umfelds und der nicht-biometrischen Datenspeicherung,
- Vorkehrungen zum Datenschutz,
- Interaktion mit der Anwendung, die auf das biometrische System zurückgreift.

Technische Schnittstellen

Im »Biometrics Tutorial« sind hier die technischen Schnittstellen zu externer Software (*Biometric Application Programming Interface* (BioAPI)) und Hardware- und Protokollschnittstellen (*Biometric Interworking Protocol* (BIP)) zur Vernetzung zwischen verschiedenen Biometriesystemen erwähnt.[136] Außerdem gehört ein Metadatenaustauschformat, (z. B. *Common Biometric Exchange Formats Framework* (CBEFF)) zu den technischen Schnittstellen eines biometrischen Systems. Die Nutzung standardisierter Schnittstellen ermöglicht eine hohe Modularität biometrischer Systeme, in denen verschiedene Komponenten unterschiedlicher Hersteller leicht austauschbar, ersetzbar und vernetzbar sind.

[134] ISO/IEC TR 24741:2007, S. 14, von Verfasserin übersetzt.

[135] Punkte übernommen aus ISO/IEC TR 24741:2007, S. 14, von Verfasserin übersetzt.

[136] Vgl. ISO/IEC TR 24741:2007, S. 14.

Auch zur Realisierung von Mensch-Maschine-Schnittstellen gibt es einen speziellen Interface-Standard, der die Steuerung von grafischen Ausgaben während des Enrolments, der Verifikation und der Identifikation ermöglicht.[137] Ansonsten existieren auf der Ebene industrieller Normen nur allgemeinere Empfehlungen zu Ergonomie oder Usability und in Verbindung mit für *User Interfaces* geeigneten Piktogrammen.[138]

Jede der in den letzten Abschnitten erläuterten Teilkomponenten greift auf verschiedene typische, aber meist spezifisch für die Erscheinungsformen von Fingeroberflächen angepasste Algorithmen zurück, deren genaue Systematisierung schwierig ist. Das Buch von Maltoni, Maio, Jain und Prabhakar gibt hier wohl den umfassendsten Überblick.[139]

2.4 Prozesse in biometrischen Systemen

In diesem Kapitel wird ein im Wesentlichen an letztgenanntem Buch orientierter Kurzüberblick über die wichtigsten in der Implementierung von Fingerbilderkennungssystemen aus Signalverarbeitung und Mustererkennung spezifisch genutzten Sensortechniken sowie einige den Algorithmen zugrundeliegenden Konzepten zur Analyse, Repräsentation, Klassifikation und Ähnlichkeitserkennung, Datenformate und Schnittstellen gegeben.

2.4.1 Datenerfassung und Sensortechnik

Um eine biometrische Charakteristik für einen Signalverarbeitungsprozess physikalisch messen zu können, muss ihr entweder zunächst geeignete Energie zugeführt werden, die durch sie spezifisch verändert wird, oder sie erzeugt selbst einen solchen Energiefluss. Die Messung muss durch für das jeweilige Signal hinsichtlich des Signal-Rausch-Verhältnisses geeignete Sensoren (*Transducer*) erfolgen, die mit Hilfe eines Analog-/Digital-Wandlers die gemessene Energie in ein repräsentatives elektronisches Signal umwandeln.[140] Dazu werden die von den Sensoren aufgezeichneten Signale ver-

[137] Vgl. ISO/IEC 19784-1:2006/Amd 1:2007.

[138] Siehe ISO/IEC TR 29156:2015, ISO/IEC 24779-1:2016 sowie ISO/IEC 24779-4:2017.

[139] Maltoni u. a. 2009. Kürzere Darstellungen ausgewählter algorithmischer Prinzipien finden sich bspw. in Yau u. a. 2013 und in verschiedenen Lexikonartikeln in Li und Jain 2009: Beispielsweise Hara 2009, Allinson 2009, Bigun 2009 oder Tian, Zhang und Cao 2009 oder in der nicht frei verfügbaren permanent aktualisierten eReference-Online-Version desselben Buchs. Einen sehr interessanten Überblick über Sensortechnik, Matching-Algorithmen und zugehörige Hersteller bietet die privat gepflegte Webseite des wissenschaftlichen Ingenieurs und Chefentwicklers bei Thomson/Atmel Jean-Francois Manguet: http://biometrics.mainguet.org/types/fingerprint/fingerprint.htm, letzter Abruf: 22.7.2017. Ferner gibt es bei verschiedenen internationalen Performanzwettbewerben Einblicke in aktuelle Algorithmen verschiedener Komponenten, siehe hierzu *Unterkapitel 3.2.1 Performanzevaluationen* (S. 92).

[140] Vgl. Setlak 2009, S. 98.

stärkt, durch einen Multiplexer auf wenige Signalverarbeitungsknoten reduziert, einer Rauschreduktion und -filterung unterzogen, abgetastet, digitalisiert und final in einen formatierten Datenstrom oder -satz zur weiteren digitalen Verarbeitung überführt.[141]

Die Sensorik zur Erzeugung eines digitalen Fingerbildes wird nach Art der Eingangsenergie unterschieden, die die *Transducer* in elektrische umwandeln. Dazu gehören mechanische, optische, elektrische, ultraschallbasierte oder thermische Transduktionsmethoden.[142]

Die für die Merkmalsaufnahme genutzte Sensortechnik wird außerdem anhand der Art der Berührung der Sensorfläche klassifiziert: Hinüberziehen des Fingers über den Sensor (*Sweep*), Auflegen der kompletten Fingerfläche auf den Sensor (*Touch*), Abrollen von einer Fingernagelseite zur anderen (*Rolled Impression*) oder berührungsloses Erfassen (*Contactless/Touchless*). *Sweep*-Sensoren sind in der Regel nur so breit wie ein Finger und besitzen nur eine ganz schmale Auflagefläche, da die Sensorik hier bis auf einen oder wenige Pixel Breite reduziert ist.

Eine weitere Klassifizierung erfolgt zusätzlich danach, wieviele Finger gleichzeitig gescannt werden: *Multi-Finger* oder *Single-Finger*. Erstere werden insbesondere von den Polizeien im hoheitlichen Bereich eingesetzt, letztere im kommerziellen Bereich in allen möglichen Anwendungskontexten von privaten Smartphones, über Laptops bis hin zur Verifikation an Kassensystemen oder Eingangstoren.

Digitalisierung mechanisch erfasster Fingerbilder

Die im *Unterkapitel 2.1.2 Manuelle Fingerabdruckerkennung* (S. 28) erwähnten Fingerabdruckkarten werden für die Verwendung in AFIS mit Papierbildscannern mit mindestens 500 ppi Auflösung digitalisiert.

Mit diversen chemischen oder optischen Hilfsmitteln sichtbar gemachte latente Abdrücke werden mit hochauflösenden Kameras fotografiert und digitalisiert. Eine andere Variante ist die kontaktlose Direkterfassung durch optische Scanverfahren, die ohne solche Hilfsmittel auskommen. Hierbei wird der Abdruck mittels Infrarotlichtbestrahlung für eine entsprechende Spektren aufzeichnende multispektrale Kamera sichtbar gemacht und sogleich digitalisiert.[143]

Sensortechnik für die Direkterfassung

Die Einteilung der Sensoren in optische, elektrische (oder auch: silikon- oder halbleitertechnikbasierte), ultraschallbasierte, thermische, druck- oder geruchsbasierte Messmethoden ist in der Literatur unterschiedlich. Zum Beispiel werden die letzteren drei

[141] Vgl. Setlak 2009, S. 98.

[142] Vgl. Setlak 2004, S. 28.

[143] Ein Produkt in diesem Bereich ist das Gerät der EVISCAN GmbH, das zur „berührungslosen Fingerspurensicherung“ eingesetzt werden kann (vgl. EVISCAN GmbH 2017).

auch manchmal unter die silikonbasierten subsumiert. Alle Verfahren verbindet die Umwandlung des aufgezeichneten Signals in elektrische Spannung durch Einsatz eines dafür geeigneten Materials mit günstigen chemischen Eigenschaften bzw. kleinster Halbleiterpixel-Sensoren. Gleich im Anschluss wird ein grober Überblick über die breite Palette an Aufnahmetechniken gegeben.

- ***Optische Sensoren*** nutzen meist Photodioden in *Complementary Metal-Oxide-Semiconductor* (CMOS)-, *Charge-Coupled Device* (CCD)-Sensoren oder *Thin-Film Transistors* (TFT), um Lichtwellen aufzuzeichnen, die sich durch unterschiedliche Reflexion, Absorption oder Diffusion an den Hautleisten und ihren Zwischenräumen charakteristisch verändern. Beispiele sind:[144]
  - Die naheliegende Nutzung *berührungsloser hochaufgelöster Digitalkameraaufnahmen* war eine der ersten, anfangs zu fehleranfälligen Methoden. Neuere Produkte werden inzwischen aber als für den Einsatz in anspruchsvollen, hoheitlichen Identifikationsanwendungen geeignet angesehen.[145]
  - Die *verhinderte Totalreflexion* (*Frustrated Total Internal Reflexion*, FTIR) ist eine typische in optischen Live-Scannern genutzte Technik. Hier wird Licht durch ein Plastik- oder Glasprisma gestrahlt, auf das der Finger aufgelegt wird. Das Licht, das an der Grenzfläche zwischen Luft und Prisma auftritt, wird nahezu total reflektiert. Die noch hinter dieser Grenzfläche austretenden dahinschwindenden (evaneszenten) Wellen werden an den aufliegenden Hautleisten teilweise absorbiert, so dass die Totalreflexion verhindert wird. Die reflektierten Strahlen werden schließlich durch eine Linse auf eine kleine Fläche lichtempfindlicher Fotodioden fokussiert. Die Hautleisten erscheinen später dunkel und die Zwischenräume hell auf dem Bild.
  - Es gibt auch *Glasfaserplatten* mit direkt angebrachten und über die gesamte Auflagefläche verteilten CMOS- oder CCD-Sensoren. Das Restlicht der angestrahlten Finger strahlt hier durch die Glasfasern ohne Linsenbündelung direkt auf die Sensoren.
  - *Elektro-optische Sensoren* haben eine Fingerauflagefläche aus einem lichtemittierenden Polymer. Wird daran eine Spannung angelegt, hat dieses je nach Berührungsart (durch eine Hautleiste oder nicht) ein unterschiedliches Spannungspotential und das Licht wird unterschiedlich stark ausgesendet. Unter der Polymerschicht befindet sich wiederum eine Schicht mit lichtempfindlichen Photodioden, die in Glas eingebettet sind.
  - *Multispektralsensoren* zeichnen die elektromagnetischen Wellen jenseits des sichtbaren Lichts auf.

[144] So nicht direkt anders angegeben, sind diese Setlak 2004 oder Maltoni u. a. 2009 entnommen.

[145] Vgl. Wiggin und Ericson 2014.

- ***Silizium-Sensoren*** oder ***Halbleitersensoren*** (***Solid-State-Sensoren***) bestehen aus vielen kleinen Sensoren (pro Pixel einer), die direkt vom Finger berührt werden und auf optische Komponenten verzichten. Sie greifen vielmehr auf unmittelbare elektrische Eigenschaften von Halbleitern zurück, indem die Leitfähigkeit in Form von Spannungs-, Stromstärken-, Widerstandsänderungen oder die Kapazität bei Berührung gemessen werden. Hierbei gibt es unzählige patentierte Implementierungen, die sich grob nach den konkret genutzten Merkmalen einteilen lassen:

  - *Kapazitive Sensoren* sind das üblichste. In einer mit einer dünnen nichtleitenden (dielektrischen) Schicht überzogenen Auflagefläche sind viele pixelgroße Mikro-Elektroden enthalten, die zusammen mit der Fingeroberfläche, die auch als Elektrode fungiert, einen Kondensator bilden. Die sich bei Berührung aufbauende Ladung variiert je nach Abstand der Haut zur Elektrode, so dass aus den verschiedenen Kapazitäten die Lage der Hautleisten gemessen werden kann. Eine Variation dieser Sensortechnik sind sogenannte Doppel-Elektroden- bzw. Differential-Kapazitätssensoren – hier wird pro Pixel die Kapazität zwischen zwei Mikro-Elektroden gemessen.[146] Die Messung erfolgt sequentiell Pixel für Pixel.

  - Die *Bilderkennung mit Hilfe elektromagnetischer Wellen* (*Radio Frequency Imaging*) läuft über einen *Drive Ring*, der ein hochfrequentes elektromagnetisches Wechselfeld erzeugt, das durch die Struktur der Haut, die ebenfalls elektrische Eigenschaften hat, moduliert wird. Das modulierte Signal mit sehr kleiner Amplitude wird von pixelgroßen aktiven Antennen, den Sensoren, gleichzeitig aufgezeichnet, verstärkt, integriert und digitalisiert. Der Finger muss sowohl *Drive Ring* und das Antennenfeld hierfür berühren. Mit dieser Methode ist es möglich, die unter der oberflächlichen Schicht bereits abgestorbener Hautzellen (zw. 0,05 bis 1,3 mm dick) liegende lebende Hautschicht zu erfassen. Diese ist weitaus weniger von Verletzungen, verschiedenen Feuchtigkeits- oder Verschmutzungszuständen der Hautoberfläche beeinträchtigt. Hierzu können Phasenverschiebungen und Frequenzen der Sensoren sowie der Sendeeinheit angepasst werden, so dass zwischen den elektrischen Signalen der oberen und unteren Hautschicht differenziert werden kann.

  - *Thermische Sensoren* nutzen die Eigenschaft pyroelektrischer Stoffe, bei einer Temperaturveränderung durch Berührung eine elektrische Aufladung zu produzieren. Die Hautleisten erzeugen eine andere Temperaturdifferenz als ihre Zwischenräume.

[146] Vgl. Setlak 2004, S. 33.

  - *Drucksensitive Sensoren* wiederum greifen auf die Eigenschaft piezoelektrischer Stoffe zurück, sich bei mechanischem Druck elektrisch aufzuladen. Eine andere Variante ist die Nutzung des piezoresistiven Effekts von Halbleitern, bei mechanischem Druck den elektrischen Widerstand merklich zu ändern.[147]

- ***Ultraschallsensoren*** Bei dieser akustischen Technik wird mit der verschieden starken Reflexion von einem Transmitter auf die Fingerhaut gesendeter Ultraschallwellen gearbeitet. Das Empfangsmodul zeichnet das für jede Art der Änderung des Widerstands gegen die Ausbreitung der Schallwellen durch die Hautpartien charakteristische Echo auf. Die Methode funktioniert auch durch Handschuhe oder Ölbeschichtungen hindurch. Es ist zudem möglich, tieferliegende Hautschichten bildlich darzustellen. Die Anfang der nuller Jahre produzierten Technologien waren große Geräte mit mechanisch betriebenen Scannern. Inzwischen ist die Technik reif für eine Implementierung in Smartphones und wird als *3D-Fingerprint Sensing* vermarktet.[148]

- ***Sensoren für die Lebenderkennung*** nutzen entweder die Möglichkeiten der bereits erwähnten Techniken aus, um neben der Detektion des Verlaufs der Papillarlinien auch Eigenschaften zu messen, von denen man hofft, auf die Lebendigkeit des Fingers zu schließen.[149] Dazu gehören das Messen elektrischen Widerstands, optischer Charakteristika wie bestimmte Arten der Lichtabsorption, -reflexion, -streuung und -brechung oder die Messung dielektrischer Durchlässigkeit. Zusätzliche Sensorik wird häufig für Hauttemperaturmessung, Pulsoximetrie oder Blutdruckmessung verwendet. Sogenannte elektronische Nasen können zudem mittels eines Felds aus chemischen Sensoren charakteristische Geruchsstoffe lebender Haut erkennen.

Viele der oben aufgezählten Technologien werden auch zu den sogenannten mikroelektromechanischen Systemen (MEMS) gezählt, insofern – wie beispielsweise bei den extrem kleinen Fingerbildscannern in Smartphones – die Transducer auf hochintegrierten Siliziumchips aufgebracht und direkt mit diesen verschaltet sind.[150]

---

[147] Vgl. Zhou, Wong und Rufer 2010.

[148] Seit 2015 hat *Qualcomm* Smartphones angekündigt, die mit der *Snapdragon Sense ID*-Technologie ausgerüstet sind, vgl. Sammons 2015 sowie Patent: Schneider, Kitchens und Baker 2013. Eine ähnliche Entwicklung im Mikrometerbereich auf Basis eines piezoelektrischen Ultraschallwandlers stammt von einem Forscherteam der *University of California*, Lu u. a. 2015.

[149] Die folgenden Varianten wurden in einem Überblick in Baldisserra u. a. 2005, S. 265 zusammengetragen, die selbst eine eigene Methode der Geruchsanalyse vorschlagen.

[150] Vgl. Setlak 2009, S. 98. Setlak weist darauf hin, dass durch diese Form der Integration von Transducern und Halbleiterschaltkreisen die Größe und Kosten von biometrischen Datenerfassungssystemen allein zwischen 1997 und 2007 um den Faktor 100 reduziert werden konnte.

Bilderzeugung

Die Analog-/Digital-Konvertierung wird entweder in die Sensortechnik integriert, oder es wird zusätzlich auf eine extra entwickelte Framegrabber-Schaltungskomponente, wie sie in Kameratechnik eingesetzt wird, zurückgegriffen.

Bevor die Gewinnung von Merkmalen für den späteren Fingerbildvergleich, die Bildanalyse, beginnt, wird zunächst ein geeignetes Bildformat erzeugt und oft als *Captured Biometric Sample* gespeichert.[151]

Folgende Prozesse können beispielsweise Teil der Bilderzeugung sein:

- Zerlegen von Bildaufnahmen mehrerer Finger in Einzelfingerbilder (*Slap Segmentation*),
- Qualitätsprüfungen der Aufnahmen (zum Beispiel mit lokalen und globalen Kontrastschätzungen),
- Zusammensetzen von Einzelaufnahmen kleiner Teile des Fingers bei kleinen Sensorflächen oder Sweep-Sensoren,
- Bildkompression.

Parameter von Fingerbildern

Durch die Festlegung bestimmter Qualitätsparameter für die Sample-Akquise soll sichergestellt werden, dass die spezifische Entropie eines Merkmals für dessen eindeutige Unterscheidbarkeit von dem gleichen Merkmal bei vielen anderen Menschen so groß wie möglich ist.[152] Die Beeinträchtigung durch die intrinsische Variabilität des Merkmals selbst, durch die Veränderlichkeit der Umgebung, durch die verschiedenen Arten der Merkmalspräsentation, durch Verletzungen oder andere Arten von Fehlern und Störungen soll so minimiert werden, dass man sich dem Ideal nähert, von ein und derselben Charakteristik stets dieselben biometrischen Daten zu erhalten.[153] Außerdem müssen Interoperabilität und Kompatibilität der mit verschiedenen Techniken erzeugten Bilder mit den restlichen Systemkomponenten und über zeitliche wie räumliche Systemgrenzen hinweg abgesichert werden.

Um geräteseitig sicherzustellen, Fingerbilder bestmöglich und gut verwertbar wiederzugeben, gibt es zahlreiche Anforderungen an Bildformate und -qualität, die Bildgröße, Auflösung, erfasste Fingeroberfläche, geometrische Präzision, Kontrast, Verzeichnung, Bittiefe, Intensitätsspanne, Uniformität und Linearität der Grauwerte, den Detailkontrastverlust durch das Sampling und das Signal-Rausch-Verhältnis betreffen.

---

[151] Siehe *Abschnitt: Bildformate und Speichertechniken* (S. 55).

[152] Vgl. Setlak 2009, S. 97

[153] Vgl. ebd.

Mit Hilfe normierter Nennwerte und zugehöriger Toleranzen für oben genannte Parameter lässt sich herstellerunabhängig eine Bildqualität absichern, die den Ablauf des biometrischen Vergleichsprozesses nicht aufgrund eines mangelhaften Samplings beeinträchtigt. Detaillierter werden wichtige Standards und Empfehlungen für die Qualität und die Datenformate digitaler Fingerbilder sowie Anforderungen an die diesbezügliche Sensortechnik sowohl im kommerziellen als auch im hoheitlichen Bereich im Abschnitt *Qualitätsanforderungen an die Bilddaten und ihre Messung* vorgestellt.

Bildformate und Speichertechniken

Die bei der Datenerfassung digitalisierten Grauwertbilder der Fingeroberfläche werden meist in üblichen, möglichst verlustfreien Datenformaten mit Metadaten versehen in einer Datenbank abgelegt.[154] Im kriminaltechnischen Bereich gelten die höchsten Anforderungen an die Bildqualität zu speichernder Samples. So wurden und werden beispielsweise beim FBI biometrische Samples mit mindestens 500 ppi Auflösung bei einer Größe von 768x768 Pixeln pro Einzelfinger mit 8 Bit Graustufen erstellt.[155] Die damit Anfang der 1990er anfallenden Datenmengen machten eine Datenkompression erforderlich, um weitere Effizienzsteigerungen bei Speicherung und Datenübertragung zu erreichen. Da es damals keinen geeigneten Kompressionsalgorithmus gab, der eine ausreichende Qualität der Bilder sicherstellte, entwickelte man einen eigenen – *Wavelet Scalar Quantization* (WSQ). Dieser basiert wie später JPEG 2000 auf der diskreten Wavelet-Transformation.[156] Da JPEG 2000 für hohe Kompressionsraten und für Auflösungen höher als 500 ppi wesentlich besser als WSQ ist, empfehlen die aktuellen Standards des *American National Standards Institute* (ANSI) und des *National Institute of Standards and Technology* (NIST) inzwischen für diese Fälle dieses Format.[157] Mit diesen Kompressionsformaten können die Graustufenbilder nahezu verlustfrei gespeichert werden.

Empfehlungen zu geeigneten kryptographischen Algorithmen zur Verschlüsselungen von Samples und Templates und zur Integration in bestehende Datenformate gibt der internationale Standard »Information technology – Security techniques – Biometric information protection« des *Subcommittee* 27 der ISO/IEC. Obwohl Biometrie bereits lange massenhaft eingesetzt wird, wurde das Dokument erst 2006 auf den Weg gebracht und 2011 veröffentlicht.[158]

---

[154] Die international akzeptierten Standard-Metadatenformate werden im Abschnitt *Standardisierte Speicher- und Austauschformate* (S. 70) kurz erläutert.

[155] Vgl. Maltoni u. a. 2009, S. 92.

[156] Vgl ebd.

[157] Vgl. ANSI/NIST-ITL 1-2011, S. 76 und Orandi u. a. 2014.

[158] Siehe ISO/IEC 24745:2011.

2.4.2 Fingerbildverarbeitung und Merkmalsextraktion

Die auf die Datenerfassung und erste Bildvorverarbeitung folgenden Prozesse, die der Verbesserung des Nutzsignals, der Reduktion des Rauschens und damit der Herauslösung der biometrischen Daten aus dem Hintergrund dienen,[159] gehen fließend in die Merkmalsextraktion über. Im Prozess der *Merkmalsextraktion* (*Feature extraction*) werden dann aus einem vorverarbeiteten biometrischen Sample die Daten berechnet, die eine wiederholbare eindeutige Zuordnung eines erfassten Musters zum „Datensubjekt" ermöglichen sollen. Die Features repräsentieren mathematisch häufig, aber nicht zwangsläufig verschiedene Aspekte der Merkmale, die auch von manuell arbeitenden Daktyloskopinnen genutzt werden.[160]

Am Anfang der also nun erforderlichen fortgesetzten Bildverarbeitung und -analyse stehen meist Pixelgrafiken, die die Ausgabe der Datenerfassung sind. Aus ihnen ist die gängige Repräsentation der Oberfläche der Fingerkuppen als zweidimensionaler Vektor G der Grauwerte gut ableitbar: $f : D_X \times D_Y \rightarrow G$. Hierbei ist G[x,y] der Grauwert g an den Koordinaten (x,y) – niedrige Grauwerte nahe 0 sind dunkel, Grauwerte nahe g−1 sind heller. Die räumliche Oberflächenstruktur S lässt sich dann diskret mittels z=S(x,y)=g−1−G[x,y] berechnen.[161] In der Visualisierung dieser Struktur in Abbildung 2.4 lässt sich gut erkennen, dass die dunkleren Werte die Hautleisten und die helleren die Rillen zwischen diesen repräsentieren.

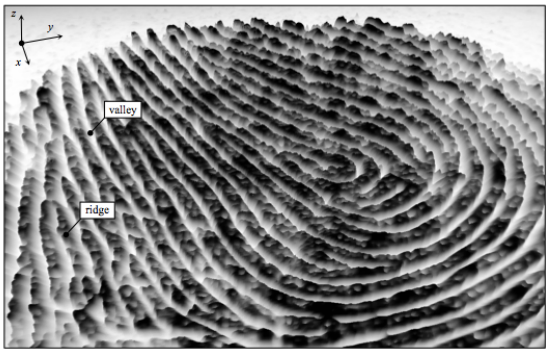


Abbildung 2.4: Oberflächenplot eines Fingerabdrucks. Abbildung aus Maltoni u. a. 2009, S. 102, © Springer-Verlag.

Maltoni et al. trennen folgende Teilschritte der Bildverarbeitung/-analyse, die verschieden implementiert oder in manchen System nur teilweise umgesetzt werden:[162]

[159] Vgl. Du 2013.

[160] Siehe hierzu *Unterkapitel 2.1.2 Manuelle Fingerabdruckerkennung* (S. 28).

[161] Vgl. Maltoni u. a. 2009, S. 102.

[162] Vgl. ebd., S. 97 ff.

- Berechnen der lokalen Ausrichtung der Papillarleisten (*Local Ridge Orientation*), die in einem sogenannten *Orientierungsfeld* (*Orientation Image*) gespeichert wird,
- Ermitteln der lokalen Dichte der Papillarleisten (*Local Ridge Frequency*), die in einem *Frequency Image* gespeichert wird,
- Segmentierung des Bildes, bei der die Fläche des Fingerabdrucks vom Bildhintergrund getrennt wird,
- Singularitäten- und Kernerkennung (*Singularity and Core Detection*), um beispielsweise das Bild auszurichten oder zu zentrieren,
- Schätzung und Verbesserung der Bildqualität (*Fingerprint Image Enhancement*),
- Minutienerkennung (*Minutiae Detection*),
- Minutienfilterung, um fälschlicherweise als Minutien erkannte Artefakte auszuschließen und
- Schätzung der Hautleistenanzahl (*Estimation of Ridge Count*).

Einige für die Fingerbilderkennung typische Schritte werden in den nächsten Abschnitten exemplarisch vorgestellt.

Lokale Ausrichtung und Dichte der Hautleisten

Für die Schätzung der Richtung der Papillarlinien, angegeben mit dem Winkel θ_{ij} ($0 \leq \theta < \Pi$), in einem Blockausschnitt des Fingerbildes der Größe $w \times w$ mit dem Zentrum [i,j] über dem Pixel [x_i,x_j] (siehe Abbildung 2.5) gibt es zwei grundlegende Herangehensweisen: das stückweise und das kontinuierliche Vorgehen.[163] Bei einer stückweisen Schätzung wird eine feste Anzahl n_s von Referenzausrichtungen R_k festgelegt: $R_k = k\frac{\Pi}{n_s}, k = 0...n_s - 1$, die einzeln für jedes Fenster durchgegangen werden.[164] Pro Ausrichtungskante werden die dort vorhandenen Grauwerte bspw. summiert, so dass die lokale Ausrichtung $\theta_{ij} = R_{k_{opt}}$ an Punkt [i,j] gewählt wird, auf der die meisten Grauwerte liegen. Bei der kontinuierlichen Schätzung werden lokale Gradienten im Fingerbild berechnet, die anschließend gemittelt werden.[165]

[163] Vgl. Yau u. a. 2013, S. 15.

[164] Vgl. Maltoni u. a. 2009, S. 106.

[165] Vgl. ebd., S. 104.

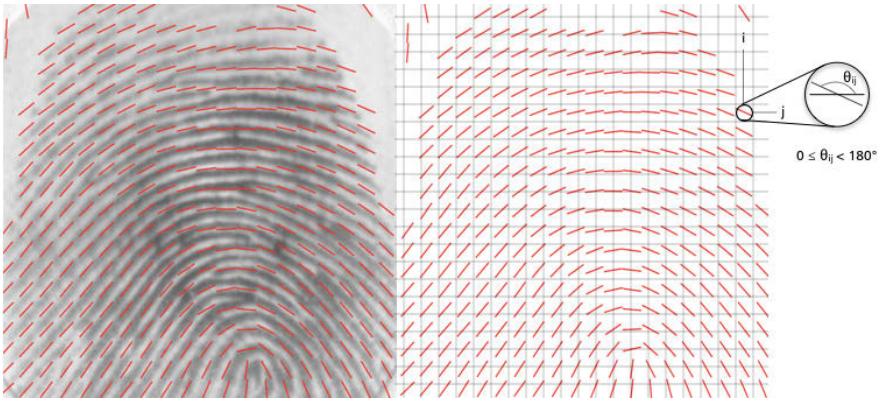


Abbildung 2.5: Fingerbild (links) mit geschätzten lokalen Ausrichtungen der Papillarlinien rechts. Für einen Punkt [i,j] in einem 15x15-Pixel-Block ist beispielhaft der Ausrichtungswinkel θ_{ij} der durch den Block verlaufenden Hautleiste visualisiert. Screenshots aus SourceAFIS 1.7, Abbildung angelehnt an Maltoni u. a. 2009, S. 103.

Um Störungen wie Flecken o. ä. im Bild auszugleichen, durch die man den Linienverlauf nicht mehr erkennen kann, werden verschiedene Ansätze der Bildglättung oder einer Gesamtmodellierung von Fingerlinienausrichtungen genutzt.[166]

Neben dem Bild der lokalen Ausrichtung der Hautleisten wird das Frequenzbild berechnet. Hierbei wird entlang eines fest definierten Segmentes mit dem Punkt [x,y] als Mittelpunkt, das senkrecht zu den Orientierungslinien verläuft, die Anzahl der Hautleisten pro Längeneinheit als lokale Frequenz f_{xy} an Punkt [x,y] berechnet. Mit Hilfe der Frequenzdarstellung (Beispiel siehe Abbildung 2.6) lassen sich charakteristische Regionen eines Fingerbildes bestimmen.

Abbildung 2.6: Rechts die Darstellung der lokalen Hautleisten-Frequenzen des linken Fingerbilds. Hohe Frequenzen sind hell. Abbildung aus Maltoni u. a. 2009, S. 113, © Springer-Verlag.

[166] Dutzende davon sind unter Maltoni u. a. 2009, S. 108 ff. zusammengefasst.

Segmentierung

Für die Ablösung des relevanten Fingerbildes vom Hintergrund kann die Tatsache benutzt werden, dass dieses ein gestreiftes und spezifisch ausgerichtetes Muster aufweist, während der Hintergrund keine dominante Orientierung besitzt. Ein naheliegender Ansatz für die Segmentierung ist daher zum Beispiel die Berechnung der Ausrichtungsstärke pro Bildblock – wenn diese unter einer bestimmten Schwelle ist, wird der Block als Hintergrund markiert (Abbildung 2.7).

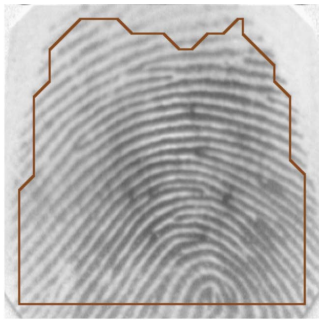


Abbildung 2.7: Die Linie zeigt das Ergebnis einer Segmentierung. Screenshot der Visualisierung von SourceAFIS 1.7.

Es gibt zahlreiche weitere Verfahren etwa unter Einbeziehung von Qualitätsschätzungen oder mit Rückgriff auf lernbasierte Ansätze.[167]

Fingerbildverbesserung

Die Verbesserung der Bildqualität soll eine klare Unterscheidung von Hautleisten und ihren Zwischenräumen in der Merkmalsextraktionsphase ermöglichen und Fehler durch Dreck auf dem Sensor, Narben, zu trockene oder zu feuchte Finger o. ä. korrigieren. Hierzu wird auf typische Bildverbesserungsstrategien wie Punkt-, Nachbarschafts- und Kontextoperationen zurückgegriffen. Abbildung 2.8 zeigt den Effekt der typischen Punktoperation der Histogrammspreizung (Normalisierung), die in Abhängigkeit von den Grauwerten der Pixel und ihrer Häufigkeitsverteilung in einem Block angewandt wird.

Am häufigsten werden zur Bildverbesserung allerdings Kontextoperationen in Abhängigkeit von der lokalen Papillarlinienausrichtung und -häufigkeit eingesetzt.[168] Dazu gehören Tiefpass- oder Bandbreitenfilter, Gabor-Filter sowie die Kurzzeit-Fourier-Transformation.[169]

[167] Siehe hierzu ebenfalls den Überblick von ebd., S. 116 ff.

[168] Vgl. Yau u. a. 2013, S. 18.

[169] Für die Beschreibung dieser Verfahren vgl. Maltoni u. a. 2009, S. 134 ff.

Abbildung 2.8: Ergebnis einer Bildverbesserung durch Histogrammspreizung. Abbildung aus Hong, Wan und Jain 1998, S. 781, © IEEE.

Singularitäten- und Kernerkennung

Die in Abbildung 2.2 gezeigten Level-1-Merkmale, insbesondere die Kerne und Deltas sind sowohl für die Bildzentrierung als auch die Mustererkennung hilfreich. Für ihre Erkennung gibt es vier gängige Verfahren. Erstens, vorgegebene Muster oder Modelle von Kernen und Deltas werden mit den aktuellen Fingerbildern verglichen.[170]

Zweitens werden durch die Singularitäten entstehende Eigenschaften globaler geometrischer Projektionen der Punkte oder Vektoren des Originalbildes bzw. des Orientierungsfeldes genutzt. Zum Beispiel schneiden sich die Normalen der Tangenten der einzelnen Orientierungslinien in der Regel nahe an einem Kernpunkt.[171] Bei der Projektion in einen Modellraum mittels Houghtransformation werden die Singularitäten ebenfalls gut sichtbar.[172]

Drittens gibt es Ansätze, bei denen das Bild anhand des Orientierungsfeldes in Regionen gleicher Ausrichtungen partitioniert wird. Die Grenzen dieser Regionen („faultlines“) konvergieren insbesondere an Singularitäten (siehe Abbildung 2.9).

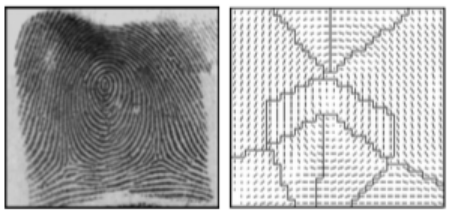


Abbildung 2.9: Fingerbild und zugehöriges in Partitionen zerlegtes Orientierungsfeld, bei dem sich die Fault-Lines an Wirbeln und Deltas kreuzen. Abbildung aus Cappelli, Lumini u. a. 1999, S. 405, © IEEE.

[170] Vgl. hier bspw. die Nutzung des *Poincaré-Index*, beschrieben bei Maltoni u. a. 2009, S. 121.

[171] Vgl. Yau u. a. 2013, S. 21.

[172] Vgl. Maltoni u. a. 2009, S. 127 f. Mit der Houghtransformation lassen sich verschiedene geometrische Figuren, deren Form bekannt ist, wiedererkennen. Das Verfahrensprinzip wird bei Jähne 2012, S. 551 ff. beschrieben.

Schließlich wird auch auf lokale Besonderheiten des Orientierungsfeldes zurückgegriffen wie zum Beispiel in einem Bild, das die Kohärenz der Richtungsvektoren in 3x3-Fenstern zeigt (siehe Abbildung 2.10). In der Nähe von Singularitäten gibt es viele Unregelmäßigkeiten, so dass die Kohärenz hier auffällig gering ist.[173]

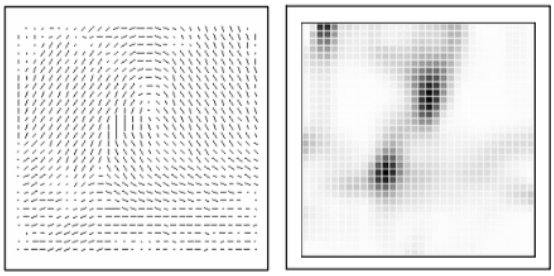


Abbildung 2.10: Orientierungsfeld eines Fingerbildes und rechts daneben das zugehörige Kohärenzbild mit niedriger Kohärenz an den dunklen Stellen, die auf Singularitäten im Fingerbild hindeuten. Abbildung aus Maltoni u. a. 2009, S. 124, © Springer-Verlag.

Häufig werden mehrere Ansätze miteinander kombiniert. Da viele Fingerbilder allerdings gar keine Singularitäten besitzen und die exakte Positionsfindung fehleranfällig ist, ist vor allem ihre zusätzliche Nutzung neben dem Orientierungsfeld in der Merkmalserkennung sinnvoll. Außerdem können sie als Prüfkriterium für den anschließenden Mustervergleich oder als Registrierungskategorie für abgelegte Fingerabdrücke genutzt werden.[174]

Minutienerkennung und -filterung

Der Mustervergleich beruht in den meisten Fingerabdruckerkennungssystemen auf den Level-2-Merkmalen, den Minutien (siehe Abbildung 2.2).[175] Die übliche Vorgehensweise für deren Erkennung teilt sich in die folgenden Schritte:

1. Binarisierung – Erstellung eines reinen Schwarz-Weiß-Bildes mittels eines Schwellwertverfahrens,
2. Skelettierung durch Ausdünnen der schwarzen Anteile auf pixelbreite Linien,
3. Suchen von Enden der Papillarlinien (*Ridge Tracing*), also Kantenenden (*Ridge Ending*) und -gabelungen (*Bifurcations*).

Dies lässt sich anschaulich anhand Abbildung 2.11 nachvollziehen.

[173] Vgl. Maltoni u. a. 2009, S. 124.

[174] Zu letzterem Punkt siehe ebd., S. 128 ff.

[175] Vgl. ebd., S. 143.

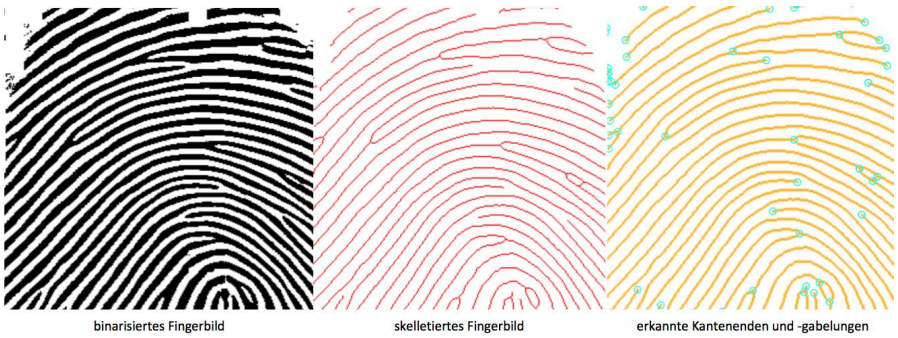


Abbildung 2.11: Grobe Schritte einer Minutienerkennung. Screenshot der Visualisierung von SourceAFIS 1.7.

Das zuletzt genannte *Ridge Tracing* wird durch einen Scan des gesamten Bildes realisiert, in dem innerhalb der 3x3-Pixel-Umgebung eines Punktes p die Anzahl der Schwarz-Weiß-Übergänge (*Crossing Number* cn(p)) benachbarter Pixel nach der folgenden Gleichung berechnet wird:

$$cn(p) = \frac{1}{2} \sum_{i=1\ldots8} |val(p_{i \bmod 8} - val(p_{i-1})|.$$

Hierbei sind p_0, p_1, ..., p_7 die acht Pixel, die im 3x3-Fenster den Punkt p umgeben, val(p)={0,1} ist der Wert eines Pixels (schwarz oder weiß). In Abbildung 2.12 sieht man, dass cn(p) mit val(p)=1 je nach Lage des Pixels an einem Kantenende, einer Gabelung oder innerhalb einer Kante einen jeweils charakteristischen Wert hat.

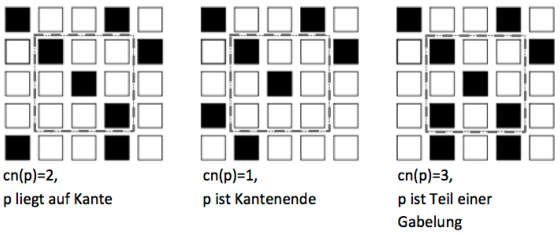


Abbildung 2.12: Einfaches *Ridge Tracing* in der 3x3-Pixel-Umgebung eines Punktes. Der hier nicht gezeigte Fall $cn(p) > 3$ bedeutet, dass es sich um eine komplexere Minutie handelt. Abbildung aus Maltoni u. a. 2009, S. 150, © Springer-Verlag.

Innerhalb dieses idealisierten Ablaufs werden für das skelettierte Bild (siehe mittleres Bild in Abbildung 2.11) diverse Reparaturmethoden (*Minutiae Filtering*/*Minutiae Post Processing*) genutzt, um „falsche Minutien“ so stark wie möglich zu reduzieren. Dazu gehören bspw. die Beseitigung falscher Lücken in den Kanten, von Poren oder Fragmenten. Mit Hilfe fester Kodierungen üblicher Minutienfehldetektionen lassen sich hier Fehler minimieren.[176]

[176] Siehe hierzu auch die Ausführungen Maltoni u. a. 2009, S. 157 ff.

Ein anderer bedeutender Ansatz der Minutienextraktion ist die *Direct Gray-Scale Minutiae Extraction*, bei der die Kanten im Grauwertbild anhand ihrer lokalen Ausrichtung nachverfolgt werden, bis sie eine andere Kante kreuzen, enden oder die Hintergrundregion erreichen.[177]

Die Minutien werden zum Schluss als Punktkoordinaten mit Richtungswinkel θ und Minutientyp jeweils als Vektor $g_k = \{x_k, y_k, \theta, m_k\}$ kodiert, wobei (x,y) die absoluten Koordinaten der Minutie, θ der Winkel und m der Minutientyp, das heißt Kantenende oder Gabelung, sind. Die Menge der Vektoren aller Minutien ist dann das Template.[178] In Abbildung 2.13 ist dies veranschaulicht.

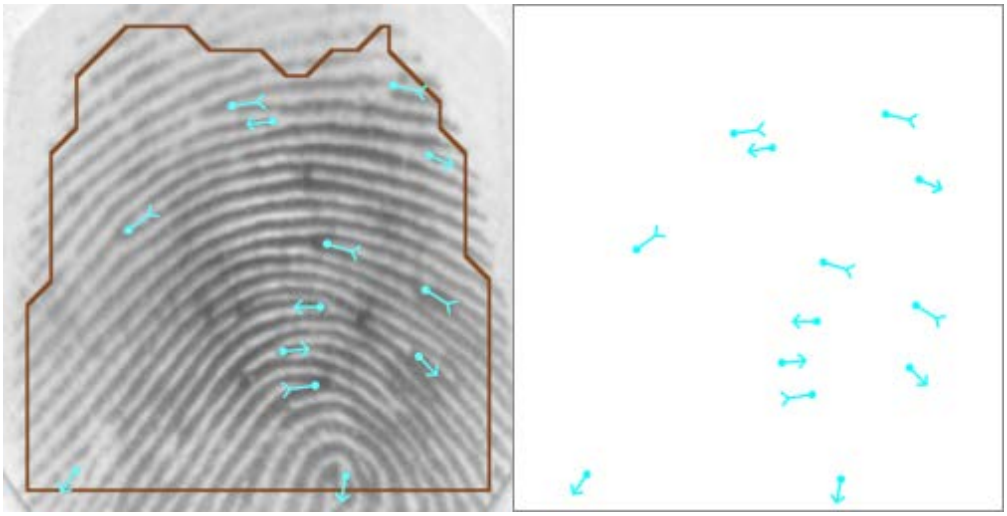


Abbildung 2.13: Die im segmentierten Bild erkannten Minutien (links) werden im Template (rechts) als Vektormenge mit ihrer Position, Richtung und ihrem Typ gespeichert. Screenshot der Visualisierung von SourceAFIS 1.7.

Schätzung der Hautleistenanzahl

Neben den oben genannten minutienbezogenen Merkmalen wird manchmal zusätzlich noch die Anzahl der Kanten, die eine Strecke zwischen zwei Punkten a und b schneidet (*Ridge Count*) als ein weiteres Merkmal genutzt, da sich damit auch die Performanz der Merkmalsextraktion erhöhen lässt.[179]

---

[177] Vgl. ebd., S. 151 ff.

[178] Der internationale Standard für die Kodierung von Templates, der die Mitte der nuller Jahre diesbezüglich noch nicht einheitlichen amerikanischen Standards harmonisiert hat, ist ISO/IEC 19794-2:2011 (erste Auflage erschien 2005).

[179] Vgl. Maltoni u. a. 2009, S. 161.

2.4.3 Ähnlichkeitserkennung und Musterklassifikatordesign

Anhand der genutzten Merkmale können vier Gruppen des biometrischen Fingerabdruckvergleichs unterschieden werden:

1. *Level-2-Matching* – Das ist *die* klassische Variante, da sie genau die Merkmale kodiert und vergleicht, die Minutien, die auch in der manuellen Daktyloskopie Anwendung finden. In groben Zügen wird eine einfache mögliche algorithmische Umsetzung daher unten genauer vorgestellt.

2. *Level-1-Matching* – Hier handelt es sich um Verfahren, die bei der allgemeinen Struktur der Papillarlinien oder ihren Orientierungsfeldern ansetzen. Sie werden oft mit Minutienvergleichsalgorithmen kombiniert, um diese etwas robuster zu machen. Zu den bekannten zählt hier der in vielen Varianten genutzte sogenannte *FingerCode*. Um ihn zu erzeugen, wird ein Fingerbild in durch ein von einem Kernpunkt ausgehenden Mosaik-Muster in Sektoren zerlegt. Diese werden einzeln mittels Gabor-Filtern, die für eine feingliedrige Texturerkennung gut geeignet sind, in ein Ortsfrequenzspektrum zerlegt, dessen Energie (lokale Amplitude) in einem Feature-Vektor, dem FingerCode, fester Größe abgelegt wird. Verglichen werden die FingerCodes, indem die euklidische Distanz der Werte des Template-FingerCodes zu denen des gerade eingelesenen FingerCode berechnet wird.

3. *Level-3-Matching* – Bei Fingerbildern, die mit mehr als 1000 ppi Auflösung erstellt wurden, ist beispielsweise der direkte Vergleich von Hautporen möglich. Die hier bekannten Verfahren können vor allem in Kombination mit den bisher genannten gute Ergebnisse erzielen.[180]

4. *Korrelationsverfahren* – Grob gesagt werden bei dieser Variante die Grauwertintensitäten korrespondierender Pixel zweier Fingerbilder global oder lokal korreliert. Bei starker Korrelation wird geschlossen, dass diese von demselben Finger stammen. Diese Verfahren sollen aber aufgrund der hohen Störanfälligkeit durch Variationen in der Fingerauflage auf dem Sensor oder Verschmutzungen u. ä. in jüngerer Zeit nicht mehr weiter verfolgt worden sein.[181]

Vergleichsalgorithmen sind meist proprietär, so dass es hier keine Standardisierung gibt.

[180] Siehe hierzu Maltoni u. a. 2009, S. 222 ff.

[181] Vgl. ebd., S. 176.

Minutiae Matching

Eine einfache mathematische Modellierung des Vergleichsproblems soll im Folgenden vorgestellt werden, um ein grundlegendes Verständnis, auf welche Weise der Vergleich digital vonstatten geht, zu ermöglichen.[182] Das Template $T = \{m_1, m_2, ..., m_m\}$ mit $m_i = \{x_i, y_i, \theta_i\}$ und $i = 1...m$ und der aus dem Eingabebild erstellte Feature-Vektor $E = \{m'_1, m'_2, ..., m'_n\}$ mit $m'_j = \{x_j, y_j, \theta_j\}$ und $j = 1...n$ stimmen dann überein, wenn die räumliche Distanz (*Spatial Distance*) *sd* zwischen ihnen kleiner ist als eine vorgegebene Abweichung r_0 und die Winkeldistanz (*Direction Distance*) *dd* zwischen den Punkten kleiner ist als eine vorgegebene Abweichung θ_0:

$$sd(m'_i, m_j) = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \leq r_0,$$
$$dd(m'_i, m_j) = min(|\theta'_j - \theta_i|, 360° - |\theta'_j - \theta_i|) \leq \theta_0.$$

Um diesen Vergleich erfolgreich durchzuführen, ist gegebenenfalls eine Ausrichtung zur Kompensation von Drehungen und Verschiebungen beim Erstellen des Eingabebildes im Vergleich zum Template nötig. Auch Vergrößern oder Verkleinern können nötige Operationen sein. Alle anderen Korrekturen jenseits von Translation und Rotation sind allerdings gefährlich. Hier sind Abbildungsfunktionen nötig, die die geometrischen Transformationen modellieren. Es bedarf zudem einer Indikatorfunktion, die entscheidet, ob die oben angegebenen Toleranzen eingehalten werden. Schließlich werden orientiert an den in den oben gegebenen Gleichungen gefundenen Distanzen zwischen zwei Minutien – in Bezug auf Ausrichtung und räumliche Distanz in den Koordinaten – diejenigen in Pärchen zusammengefasst, die innerhalb der Toleranzdistanzen r_0 und θ_0 liegen. In Abbildung 2.14 wird dies illustriert.

Zuletzt wird die Anzahl der passenden Minutien k in einen Ähnlichkeitswert (*Similarity Score*) umgerechnet. Hierzu wird die Anzahl der Pärchen durch die durchschnittliche Anzahl der Minutien in E und T dividiert:

$$score = \frac{k}{(n+m)/2}.$$

Das ist die einfachste Herangehensweise, die etwa durch Einbeziehung der Qualität der Minutien in Form von verschiedenen Gewichtungen verfeinert werden kann.

Klassifizierung und Indizierung in Large-Scale Databases

In AFIS-Anwendungen, die der (negativen) Identifizierung unbekannter Personen dienen, sind Millionen von Referenzdatensätzen abgelegt, mit denen ein Testdatensatz abgeglichen werden muss. Um hier den Suchaufwand zu minimieren, werden Klassifikations- oder Indizierungsstrategien angewandt. Im kriminalistischen Bereich

[182] Die Darstellung fasst die Ausführungen unter ebd., S. 177 ff. zusammen. Für weitere Verfahren, die auf *Point-Pattern-Matching*-Methoden, Houghtransformation oder Anwendungen algebraischer Geometrie gegründet sind, sei ebenfalls auf diese Quelle verwiesen.

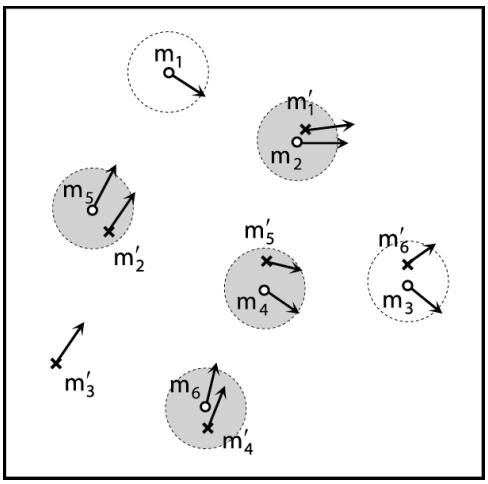


Abbildung 2.14: Die Minutien m'_n des Eingabevektors E werden auf die Koordinaten der Minutien m_m von T abgebildet. Die Kreise stellen die maximale erlaubte Distanz dar. Graue Kreise sind erfolgreich gepaarte Minutien. m_1 von T und m'_3 von E haben keinen Partner, m_3 und m'_6 haben zu starke Abweichung in ihren Ausrichtungen und sind daher kein Pärchen. Abbildung aus Maltoni u. a. 2009, S. 180.

haben sich traditionell für die manuelle Tätigkeit abgewandelte Formen der Galton-Henry-Klassifizierung etabliert, die Fingerabdrücke nach den Level-1-Merkmalen in wenige Klassen einteilen: *linke/rechte Schlinge* (*Left/Right Loop*), *Bogen* (*Arch*), *Zeltbogen* (*Tented Arch*) und *Wirbel* (*Whorl*) oder *Kompositionen* (*Composites*) hieraus.[183]

Außerdem gibt es regel-, syntax-, strukturbasierte Klassifikatoren sowie auch hier Ansätze aus Statistik, Neuronalen Netzen oder *Multiclassifier Systems* (MCS).[184]

Fehlklassifizierungen mehrdeutiger Bilder lassen sich vermeiden, indem Indizierungsmethoden genutzt werden, bei denen die Referenzdatenbank mittels numerischer Vektordarstellungen in eine Reihenfolge gebracht wird (*Continuous Classification*). Der Feature-Vektor der biometrischen Abfrage muss nun lediglich mit den Referenzvektoren verglichen werden, die nahe an ihm liegen.[185]

2.4.4 Biometrie und Maschinenlernen

Mustererkennung beinhaltet stets Optimierungsprobleme. Für die Repräsentation der erfassten Daten müssen mathematische Beschreibungen gefunden werden, die bestimmte Muster am besten approximieren. Um die Muster zu kategorisieren, müssen zudem die Parameter des Klassifikators geeignet abgeschätzt werden. Hier hat die Bio-

[183] Siehe auch *Unterkapitel 2.1.2 Manuelle Fingerabdruckerkennung* (S. 28).

[184] Vgl. Chen und Fondeur 2009, S. 67.

[185] Vgl. ebd.

metrie zwangsläufig eine große Schnittmenge mit dem Bereich der Künstlichen Intelligenz oder dem Maschinenlernen.

Ein typisches Anwendungsfeld ist hier insbesondere die automatische Selbstanpassung der Performanz eines Mustererkennungssystems. Vor allem gehört das sensorspezifische Training bestimmter Modellparameter in den Algorithmen der Merkmalsextraktion und des Vergleichs hierzu.

Die statistische Herangehensweise ist hier die am stärksten ausgeprägte Tradition. Bayes-Klassifikatoren werden sowohl in der Minutienerkennung, aber vor allem auch in der Kategorisierung großer Datenmengen von Fingerabdrücken, wie sie in Identifaktionsszenarien anfallen, eingesetzt. Stark beschädigte Bilder können mit durch Beispielfingerabdrücke trainierten *Markov Random Fields* restauriert werden.[186] Lineare Klassifikatoren für eine geeignete Segmentierung können in einem *Supervised-Learning*-Prozess mit den besten Parametern für die konkrete Anwendung versehen werden.[187] Andere Ansätze sind die Nutzung von *Support Vector Machines* (SVM), zum Beispiel für die Optimierung der Klassifizierung des am Ende berechneten Vergleichswerts zweier Muster.[188] Weitere vielversprechende Ansätze aus dem Maschinenlernen im Bereich biometrischer Techniken sind *Boosting* oder MCS.[189]

Inzwischen spielt auch die Verwendung konnektionistischer Modelle in Fingerabdruckerkennungssystemen eine wichtige Rolle. Zwar ist Mustererkennung eng mit der Forschung über neuronale Netzwerke verwandt, aber es bestehen Unterschiede in den Modellzielen, der Modell- und Rechenkomplexität, der Art der Abarbeitung der Trainingssets und der Zuverlässigkeit.[190] Beiden Ansätzen liegt zugrunde, dass sie induktiv arbeiten, wobei der klassische Mustererkennungsansatz bereits ein festgelegtes induktives Prinzip für Design und Modellierung der Klassifizierer nutzt und innerhalb neuronaler Netzwerke die Lernmethode erst kreiert wird und eine konstruktive Implementierung des induktiven Prinzips darstellt.[191]

Lumini et al. sehen mehrere Gründe, wieso die in den vorherigen Kapiteln beschriebenen traditionellen Techniken möglicherweise durch Ansätze des Maschinenlernens ersetzt würden: zum Erkennen (1) versteckter Beziehungen und Korrelationen zwischen den Daten und (2) am stärksten unterschiedlicher Features, (3) zum Umgang mit menschlich nicht mehr kodierbaren großen Datenmengen und (4) zum Berücksichtigen von Charakteristika, die zur Entwurfszeit des Systems nicht unbedingt vollständig bekannt seien.

---

[186] Vgl. Maltoni u. a. 2009, S. 110.

[187] Vgl. ebd., S. 119.

[188] Vgl. ebd., S. 181.

[189] Vgl. Lumini, Nanni und Maltoni 2010.

[190] Siehe hierzu Cherkassky, Friedman und Wechsler 1994.

[191] Siehe hierzu ausführlich Rosenfeld und Wechsler 2000, S. 101–10.

Als Nachteile trainierter oder sich trainierender Systeme benennen sie zum einen die Schwierigkeit repräsentative Trainingssets zusammenzustellen, die definitiv richtig sind und somit realistische Referenzdaten bieten. Zum anderen besteht die Gefahr eines „Overtraining" der Systeme, wenn diese so gut auf das Trainingsset abgestimmt sind, dass sie bei neuen Daten auffällig schlechter werden.[192]

2.4.5 Technische Schnittstellen eines Biometrie-Systems

Die technischen Schnittstellen eines Biometriesystems werden unterschieden nach Schnittstellen:

- *zwischen den einzelnen Komponenten* (*Inter-Component Interfaces*),
- *in einem verteilten biometrischen System* (*Intra-System Interfaces*) und
- *zwischen verschiedenen biometrischen Systemen* (*Inter-System Interfaces*).[193]

Außerdem gehören Schnittstellen zu anderer Software und für die Interaktion menschlicher Akteure mit dem System dazu.

Die technischen Schnittstellen werden mittels *Application Programming Interface* (API), Hardware- oder Protokollschnittstellen realisiert. Typische Hardwareschnittstellen für das *Data Capture Device* (*Datenerfassungsgerät*) sind heutzutage USB oder IEEE 1394 (FireWire). Für die Bilderfassung durch Scanner oder Digitalkameras beispielsweise wird häufig das TWAIN-Protokoll mit unterstützt. Zudem sind Treiber für biometrische Geräte betriebssystemabhängig notwendig.[194] Essentiell sind außerdem die Benutzungsschnittstelle sowie die entsprechenden Schnittstellen zwischen *biometrischem Betriebspersonal* (*Biometric Operational Personnel*) und Administrationssubsystem des Gesamtsystems.

Software-Schnittstellen lassen sich in einem proprietären System in der Regel mittels eines vom entsprechenden Hersteller mitgelieferten *Software Development Kit* (SDK) (heutzutage häufig in C++, C#, Java, .Net, aber auch in C) in Fremdapplikationen integrieren und beeinflussen. So kann die Biometrie-Software in einer beliebigen Applikation eingebunden werden, zum Beispiel als Teil eines Authentifizierungsmechanismus. Beispiele sind das *VeriFinger SDK* von Neurotechnology,[195] das viele handelsübliche, billigere Fingerabdruckscanner unterstützt; das SDK von Dermalog, das u. a. den Zugriff auf die in deren Software implementierte Bildqualitätskontrolle, *Fake-Finger-Detection*-Funktion oder die Unterstützung aller gängigen Bildformate in Bezug auf die

[192] Vgl. Lumini, Nanni und Maltoni 2010, S. 340.

[193] Vgl. Tilton 2009, S. 91.

[194] Vgl. ebd., S. 92.

[195] http://www.neurotechnology.com/verifinger.html, letzter Abruf: 22.7.2017.

eigenen Geräte (wie zum Beispiel den in öffentlichen Verwaltungen eingesetzten LiveScanner ZF1) ermöglicht.[196] Für nicht-kommerzielle Zwecke frei verwendbar ist beispielsweise das SDK für den Merkmalsextraktions- und Vergleichsalgorithmen umfassenden *Minutia Cylinder-Code* (MCC) von Cappelli, Ferrara, Maltoni und Maio an der Universität Bologna.[197] Es handelt sich dabei um eine .Net-DLL (Bibliothek), mit der sich Applikationen entwickeln lassen, die für Fingerabdruckverifikation auf den MCC zurückgreifen können. Ein weiteres auch als kommerziell verwendbare Open-Source-Software nutzbares SDK ist *SourceAFIS*, das eingehend im *Unterkapitel 3.7.1 Learning By Coding: Open-Source-Fingerabdruckerkennung* (S. 125) vorgestellt wird.

Wenn in einem SDK *standardisierte Schnittstellen* wie etwa die des im Folgenden näher vorgestellten BioAPI angeboten werden, wird es auch als sogenannter *Biometric Service Provider* (BSP) betrachtet.[198] BSP sind demnach Programme eines oder mehrerer verschiedener Hersteller, die Datenerfassung, Vergleich, Speicherung oder Signalverarbeitung realisieren und nach den Spezifikationen der BioAPI Zugriff auf diese erlauben. Sowohl die „High level"-Funktionen *Enroll*, *Verify* oder *Identify* als auch „Low-level primitives" wie *Capture*, *Create Template*, *Process (Feature Extraction)*, *Verify Match* usw. sind vorgesehen (Architektur siehe Abbildung 2.15).[199] Zum Beispiel bietet das SDK von Neurotechnology mittels BioAPI Zugriff auf Komponenten wie den *Fingerprint Extractor*, *Fingerprint Segmenter*, *Fingerprint Biometric Standard Support* (Umsetzung verschiedener Template- und Bildformat-Standards) und *Fingerprint Matcher* aus anderen Applikationen heraus – von der betrieblichen Zugangskontrolle, über das Login am Rechner bis hin zum AFIS.

Für das BioAPI sind zudem Datenbank-, Geräte- und biometrische Operationen, Komponentenmanagementfunktionen, Daten- und Eventhandling, Rückmeldung- und Ereignisoperationen definiert. Außerdem gibt es Konformanzkategorien, die die Funktionen und Parameter verschiedenen Produktklassen zuordnen.[200] Darüber hinaus werden die Submodule von einer Registrierungskomponente verwaltet. Eine dynamische Einfügung und Registrierung von BSPs und Geräten verschiedener Anbieter und auch ihr gleichzeitiger Betrieb sind damit möglich.[201] Das *Service Provider Inter-*

---

[196] http://www.dermalog.com/pdf/SDK_Einzelseiten.pdf, letzter Abruf: 22.7.2017.

[197] Vgl. Cappelli, Ferrara, Maltoni u. a. 2015.

[198] Das BioAPI wurde zuerst im Jahr 2000 als *Open Systems Industry Specification* von mehr als 100 Organisationen aus Industrie, Regierung und Wissenschaft, dem *BioAPI Consortium*, dann in Version 1.1 als Standard des *InterNational Committee for Information Technology Standards* (INCITS) in den USA und in Version 2.0, inzwischen auch 2.1, schließlich durch die ISO/IEC veröffentlicht. Die entsprechende Dokumentreihe ist »ISO/IEC 19784 – Information Technology – Biometric Application Programming Interface«.

[199] Vgl. Tilton 2009, S. 93.

[200] Vgl. ebd.

[201] Vgl. Nuppeney 2007.

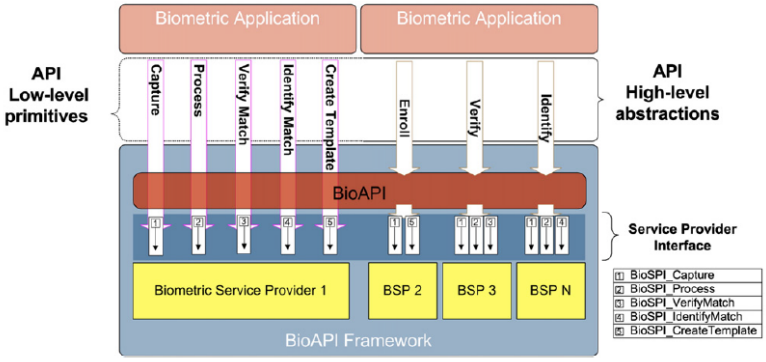


Abbildung 2.15: Schema der BioAPI-Architektur aus dem *Biometrics Tutorial*; Abbildung aus González-Agulla u. a. 2009, S. 187, © Elsevier B.V.

face (SPI) dient nun der Delegation der Aufrufe der Anwendungen über die im Framework enthaltenen Registrierungskomponenten.[202] Das BioAPI ist auch für verteilte Systeme ausgelegt, muss aber hier für erweiterte Funktionalität zusätzlich auf das *Biometric Interworking Protocol* (BIP) zurückgreifen.[203] Ein Standalone-System ist sogar eher untypisch: „Biometric systems are characterized by the fact that essential functional components are usually dislocated."[204]

Standardisierte Speicher- und Austauschformate

Wichtige Datenaustauschformate, die die biometrischen Daten so kapseln, dass sie in herstellerübergreifenden und vernetzten Systemen übertragen und verarbeitet werden können, sind das *Common Biometric Exchange Formats Framework* (CBEFF), das *Biometric Data Interchange Format* des ISO/IEC JTC 1 SC37[205] und auch das *Data Format for the Interchange of Fingerprint* des *Information Technology Laboratory* (ITL) des NIST, das CBEFF-Konformanz beinhaltet, indem es ein Extrafeld für dieses Format vorhält (*Type-99 Record*).[206] Hier sollen die ISO/IEC-Standards kurz vorgestellt werden. Abbildung 2.16 zeigt die verschiedenen Ebenen der technischen Schnittstellenspezifikationen des ISO/IEC JTC 1 SC 37.

[202] Vgl. Nuppeney 2007.

[203] Vgl. ISO/IEC 24708:2008.

[204] Busch und Canon 2009, S. 81.

[205] Spezifiziert in den Dokumentreihen »ISO/IEC 19785 – Information Technology – Common Biometric Exchange Formats Framework« sowie »ISO/IEC 29794 – Information Technology – Biometric Sample Quality« bzw. »ISO/IEC 19794 Information Technology – Biometric Data Interchange Format«. Auch das CBEFF war ursprünglich zuerst ein Standard des INCITS (Nr. 398).

[206] Vgl. ANSI/NIST-ITL 1-2011.

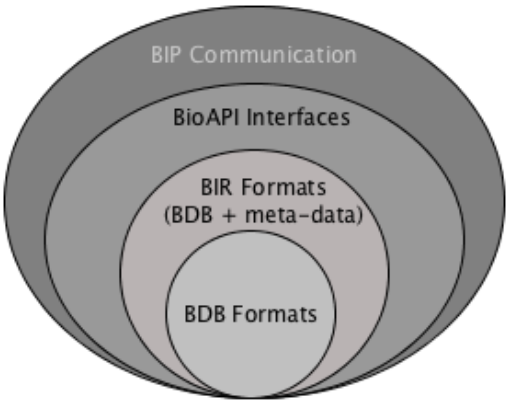


Abbildung 2.16: Auf die technischen Datenformat- und Schnittstellenspezifikationen reduziertes *Layered Model of Biometrics Standards*. Abbildung nach ISO/IEC TR 24741:2007, S. 29, © ISO/IEC.

Im Rahmen des CBEFF ist das Container-Datenformat *Biometric Information Record* (BIR) definiert. Der BIR wird in den meisten internationalen Standards als Speicher- und Transporteinheit zwischen den Software-Modulen und Computersystemen genutzt – sowohl innerhalb eines Biometriesystems in Rückgriff auf die BioAPI-Schnittstellen als auch zwischen verschiedenen Systemen unter Nutzung des BIP,[207] beispielsweise in dezentralisierten Datenbanksystemen. Ein BIR setzt sich zusammen aus einem *Biometric Data Block* (BDB), einem *Standard Biometric Header* (SBH) und optional einem *Security Block* (SB). Die biometrischen Daten sind im BDB eingebettet. Einige hierzu gehörende Attribute wie Modalität, Format, Aufnahmedatum, -geräte, -verschlüsselung, Gültigkeitsdauer und mehr werden als Metadaten im SBH hinterlegt, so dass Applikationen aus dem BIR Informationen über die biometrischen Daten entnehmen können, ohne diese selbst verarbeiten zu müssen. BDB-Formateigentümer und -typ identifizieren die Formatspezifikation, mit dem die biometrischen Daten kodiert sind, eindeutig mit 32 Bit großen Identifikatoren. Die ersten 16 Bits – Formateigentümer – werden durch eine *Registration Authority*[208] als eindeutige Kennung an eine biometrische Organisation vergeben, die für ein biometrisches Objekt wie einem BDB, dessen *Encoding* mit einem bestimmten Template-Format (*Patron Format*), Security Blocks, Produkte oder Geräte verantwortlich zeichnet. Die zweiten 16 Bits – Format-

[207] Vgl. ISO/IEC TR 24741:2007, S. 18 f.

[208] Siehe http://www.ibia.org/cbeff, letzter Abruf: 22.7.2017. Die *International Biometrics and Identity Association* (IBIA) ist eine internationale Interessenvertretung der Biometrie-Industrie, die vor allem in den USA aktiv ist. Mit Billigung des Rats der ISO/IEC kann sie als Registrierungsstelle für eindeutige Kennungen von Biometrieprodukten auftreten.

typ – kann diese Organisation selbst vergeben.[209] Im optionalen SB können Angaben zu Zertifikaten, Schlüsseln, Signaturen des BDB oder BIR gemacht werden. Der BDB kann verschlüsselt werden, der SBH nicht, wenngleich dies nicht für eine Verschlüsselung bei der Datenübertragung gilt.[210]

Für den BDB sind in der ISO/IEC-19794-Reihe verschiedene Repräsentationsarten von Fingerabdruck-, Gesichts-, Iris-, Unterschrifts-, Venen-, Handgeometrie-, Stimm-, DNA- und Handflächendaten spezifiziert. Für Fingerbilder in verschiedenen Verarbeitungsformen – Rastergrafiken, Minutien, Frequenzspektren, skelettierte Fingerbilder – gibt es allein vier eigene Dokumente. Dies ist auch dem Umstand geschuldet, dass die Kodierung der biometrischen Daten sehr unterschiedlichen Anforderungen genügen muss. Dazu gehören etwa die zügige Verarbeitung auf verschieden schnellen Prozessoren (evtl. sogar direkt auf einer Smartcard) mit möglicherweise äußerst wenig Speicherplatz (auf RFID-Tokens nur 72KB) sowie volle Interoperabilität.[211]

2.5 Fehlerbegriffe

Die Fehler der Systeme zur automatischen Wiedererkennung von Menschen anhand ihrer Fingerabdrücke stehen im Mittelpunkt dieser Untersuchung. Der Begriff *Fehler* dient hierbei als analytische Kategorie, mit der die verschiedenen Ebenen konzeptueller Brüche und Dysfunktionalitäten in der Auseinandersetzung um biometrische Fingerabdruckerkennungssysteme herausgearbeitet werden können.

Fehler sind von etwas regelhaft Beschreibbarem abweichende Zustände oder Verläufe. Sie sind Störungen in Bezug auf ein Ordnungssystem, das Prozesse in Raum und Zeit in einer bestimmten Art und Weise strukturieren soll. Fehler laufen bestimmten Anforderungen eines Systems zuwider, sind ebenso dynamisch wie sich letztere innerhalb eines sich verändernden Kontexts wandeln. Martin Weingardt, der als Erziehungswissenschaftler eine transdisziplinäre Fehlertheorie entwickelt hat, definiert in seiner Rahmentheorie des Fehlers denselben entsprechend weit und vor allem subjektbezogen:

> „Als Fehler bezeichnet ein Subjekt angesichts einer Alternative jene Variante, die von ihm – bezogen auf einen damit korrelierenden Kontext und ein spezifisches Interesse – als so ungünstig beurteilt wird, dass sie unerwünscht erscheint."[212]

Der Fehler ist somit ein Urteil, das in Wechselwirkung mit einem Kontext gefällt wird. Mit wachsender Komplexität und Dynamik des Kontexts steigt die Wahrscheinlichkeit, „dass bei wechselnden Stand- und Zeitpunkten verschiedene Beurteiler zu einer

[209] Vgl. Podio und Herr 2009, S. 184.

[210] Vgl. ebd., S. 183.

[211] Vgl. Busch und Canon 2009, S. 82.

[212] Weingardt 2004, S. 292.

widersprüchlichen Kennzeichnung erwünschter und unerwünschter Varianten kommen, und desto untauglicher wird eine feststehende normative Fehlerbeschreibung."[213]

Fehler lassen sich als Teil von *Problemen* sehen, die es so zu lösen gilt, dass die Fehler beseitigt oder minimiert werden. Probleme sind schwer oder komplex klassifizierbare Hindernisse beim Erreichen eines gewünschten Zielzustandes oder -ablaufs. Sie bedürfen einer Lösungsstrategie, können vielleicht als Kompromiss von vielen sich gegenseitig bedingenden Faktoren gemildert werden. Der Lösungsweg ist aber häufig nicht sofort klar. Fehler dagegen sind qualitativ genauer spezifizierte Problemkategorien, die sich erwartbar wiederholen und teilweise, insbesondere in Messtechnik und Statistik, quantitativ geschätzt werden können. Sie sind als Teil technischer Systeme unvermeidlich und erscheinen, wenn sie vorhersagbar oder zumindest erwartet und schätzbar sind, als kontrollierbare Abweichung eines idealisierten Systems. Sie können nach definierten Verfahren abgefangen/ignoriert, abgeschwächt oder aber auch von Vornherein vermieden werden. Auf diese klar eingrenzbare Art von Fehlern bleibt die Arbeit allerdings nicht beschränkt, sondern epistemologische und gesellschaftliche Probleme werden in die Betrachtung als weitere Fehlerkategorien einbezogen.

Ohne das Bezugssystem, innerhalb dessen bestimmte Aktionen erwartet werden, sind Fehler oder Probleme nicht näher bestimmbar. Einige übliche Fehler- und Problemtypen, die in verschiedenen Zusammenhängen und je nach Perspektive auftreten, sind:

- unerwartete Fehler (z. B. in der Softwaretechnik: Speicher- oder Rechenfehler durch ungeeignete Datentypen oder nicht abgefangene, unerwartete Eingaben);[214] erwartete Fehler (z. B. Fehler 1. und 2. Art in der Statistik; zufällige, schätzbare Messabweichungen; in der Softwaretechnik: z. B. erwartete, aber unerwünschte Fehleingaben, die mit einer spezifischen Ausnahmebehandlung abgefangen werden),
- menschliches Versagen (z. B. durch eine Fehlentscheidung der Pilotin ausgelöster Flugzeugabsturz); technisches Versagen (z. B. durch defekte Messinstrumente oder Rechenfehler im Bordcomputer ausgelöste Flugzeugkatastrophen),
- Fehler im Verhältnis zu Norm/Erwartung/Wahrheit in Bezug auf moralische Verhaltensregeln oder normative Setzungen (z. B. strafrechtlich relevantes Fehlverhalten; Sünde im Christentum),
- Fehler im Beweis einer Theorie, in der Logik einer Argumentation, auffindbar durch Falsifikation als wissenschaftliche Methode zur Validierung einer Theorie

[213] Ebd.

[214] Ein als *unerwarteter Fehler* spezifiziertes Ausnahmeverhalten bei der Ausführung eines Programms ist ein aufgeschobenes Problem. Es ist unklar, warum das Programm an dieser Stelle abstürzt. Durch nebenläufige Prozesse und Abfangmechanismen kann diese Fehlerkategorie allerdings so abgefangen oder ignoriert werden, dass nicht die gesamte Programmausführung gestoppt wird.

oder Hypothese (Teil ihrer Widerlegung/Unbrauchbarmachung) oder aber durch Kritik/Dekonstruktion als wissenschaftliche Methode der gezielten Infragestellung von Begriffen (z. B. negative Dialektik),

- Fehler als didaktische Lernhilfsmittel, wie sie im *Lernen aus Fehlern*, aber auch als evaluative wissenschaftliche und betriebswirtschaftliche Methode genutzt werden (z. B. Psychologie, Ursachenforschung Medizin, Fehlermanagement),
- Probleme als komplexe Aufgabenstellungen, die mit problemorientiertem/-lösendem Lernen und Entwerfen kreativ zu lösen sind, da sie (noch) keinen schematisch idealisierten Lösungsweg beinhalten,
- die meisten praktischen Alltagsprobleme (z. B. Douglas Adams' rotes Sofa).[215]

Diese Aufzählung soll illustrieren, auf welch verschiedenen Ebenen ein Diskurs über Fehler stattfinden kann. Die gesellschaftliche Auseinandersetzung über die Probleme von Fingerabdruckerkennungstechnologien läuft ähnlich durcheinander. In Diskussionen in Wirtschaft und Politik wirken die Abwägungen des Fürs und Widers derartiger Techniken in einer anderen Systematik zusammen als in einer rein disziplinären Auseinandersetzung um spezifische Performanz- oder Überwindungsfehler, die schon stark normiert sind, um sie handhabbarer zu machen und die nur noch abgeschwächt in das argumentative Gewimmel rückkoppelt. In dieser Arbeit sind genau die speziellen Strukturmerkmale dieser Rückkopplung von Interesse – und insofern sind die einbezogenen Perspektiven auf mögliche Fehler von Fingerabdruckerkennungssystemen auch entsprechend weit gefächert und werden im *Teil 3 Forschungsstand: Fehler von Fingerabdruckerkennungssystemen* in fünf Gruppen (Kapitel 3.2 bis Kapitel 3.6) gegliedert und in ihrer Strukturierung mit den zu beachtenden Entwurfskriterien im Systemdesign in Beziehung gesetzt.

An dieser Stelle sollen bereits die wichtigsten Begriffe als erste Orientierung kurz genannt und definiert werden, wenngleich sich zeigen wird, dass sie in der Literatur uneinheitlich erklärt werden. Die fünf aufgezählten „Fehlergruppen" steigen gewissermaßen – in Bezug auf Weingardt – in ihrem Komplexitätsgrad an. Während die erste Gruppe noch ein stark abstrahierte und objektivierte, technisch normative Sicht auf die Fehler darstellt, ist die letztgenannte bereits eine alle anderen umfassende perspektivengebundene, analytisch schwer eingrenzbare Gesamtsicht auf unerwünschte Effekte von Fingerabdruckerkennungssystemen in der Gesellschaft. Diese erste Taxonomie wird im Rahmen dieser Arbeit als produktive und zu entwickelnde betrachtet:

[215] Im ersten Kriminalroman von Adams gibt es dieses Sofa, das sich bei einem Umzug zufällig so im Treppenhaus verklemmt, dass es keinen Millimeter mehr vor oder zurück zu bewegen ist. Auch acht Macintosh-Rechner, die mehrere Jahrmillionen gleichzeitig an dem Problem rechnen, finden nicht heraus, wie man das Sofa je wieder bewegen könnte, ohne nicht das gesamte Treppenhaus zu zerstören (vgl. Adams 1987).

1. *Quantifizierte und formalisierte Fehler*:

   - *Systemfehler/Performanzraten*:[216]

     – *False Match* (*Falschübereinstimmung*): ist die Entscheidung nach einem biometrischen Vergleich, dass von zwei verschiedenen Personen stammende biometrische Referenzen übereinstimmen. Der Anteil der falschen Übereinstimmungen an der Gesamtzahl aller Vergleiche ist die *False Match Rate* (FMR).

     – *False Non-Match* (*Falschnichtübereinstimmung*): ist die Entscheidung nach einem biometrischen Vergleich, dass verschiedene von ein und derselben Person stammende biometrische Referenzen nicht übereinstimmen. Der Anteil der falschen Nichtübereinstimmungen an der Gesamtzahl aller Vergleiche ist die *False Non-Match Rate* (FNMR). FMR und FNMR bedingen einander.[217]

     – *False Acceptance* (*Falschakzeptanz*): ist auf die konkrete Anwendung bezogen die falsche Bestätigung einer biometrischen Behauptung durch die Systementscheidung (z. B. in einem Watchlist-System: „Ich bin nicht die gesuchte Person XY“, ist die biometrische Behauptung, obwohl die Person in Wahrheit XY ist. Bestätigt das System die Behauptung, handelt es sich um eine falsche Akzeptanz). Der Anteil an Falschakzeptanzen an der Gesamtzahl aller Prüfungen biometrischer Behauptungen ist die *False Acceptance Rate* (FAR) – hier wird die *Failure-to-Acquire Rate* (siehe unten) einbezogen.

     – *False Rejection* (*Falschrückweisung*): ist auf die konkrete Anwendung bezogen die falsche Ablehnung einer biometrischen Behauptung durch die Systementscheidung (z. B. in einem Watchlist-System: „Ich bin nicht die gesuchte Person XY“, ist die biometrische Behauptung, und die Person ist auch in Wahrheit nicht XY. Lehnt das System die Behauptung ab, handelt es sich um eine falsche Zurückweisung). Der Anteil an Falschrückweisungen an der Gesamtzahl aller Prüfungen biometrischer Behauptungen ist die *False Rejection Rate* (FRR) – hier wird die *Failure-to-Acquire Rate* (siehe unten) einbezogen.

[216] Die folgenden Definitionen sind in der Literatur und teilweise auch in den ISO/IEC-Standards nicht konsistent. Die hier angegebenen Varianten für *False Match*/*False Non-Match* sind ISO/IEC 2382-37:2017 entnommen; *False Acceptance*/*False Rejection* sind an Maltoni u. a. 2009, S. 15 angelehnt und konform mit der Definition in ISO/IEC 2382-37:2017, aber nicht mit der in ISO/IEC 19795-1:2006 – dort werden diese Raten nur für Verifikationsanwendungen genutzt. Alle anderen Definitionen sind an ISO/IEC 2382-37:2017 orientiert.

[217] Siehe hierzu *Abschnitt: Erkennungs- und Vergleichsfehlerraten* (S. 97).

  - *Failure to Capture* (FTC, *Erfassungsfehler*): Fehler, ein biometrisches Sample bei der Erfassung zu erstellen. Der Anteil der Fehler an der Gesamtzahl aller Erfassungsversuche ist die *Failure-to-Capture Rate*.
  - *Failure to Acquire* (FTA, *Akquisitionsfehlfunktion*): Falls ein biometrisches Sample erfolgreich erstellt wurde, das sich aber nicht weiter verarbeiten lässt, weil es den systembezogen definierten Qualitätsanforderungen nicht genügt, tritt eine Akquisitionsfehlfunktion auf. Der Anteil der Fehler an der Gesamtzahl aller Akquisitionen ist die *Failure-to-Acquire Rate* (FTAR).
  - *Failure to Enrol* (FTE): Fehler, einen Enrolmentdatensatz gemäß Systemregeln zu kreieren und zu speichern. Der Anteil der Fehler an der Anzahl aller Enrolmentversuche ist die FTER.
  - Weitere Leistungskenndaten sind u. a. *Throughput*, *False-Negative Identification-Error*, *False-Positive Identification-Error* oder *Pre-Selection Error*, die aber deutlich seltener verwendet werden.[218]

- *Konformanzfehler*: Fehler, die durch Nicht-Einhaltung bestimmter Normen entstehen; zum Beispiel falsche Datenformate, falsche Prozessabläufe bei Qualitätsprüfungen o. ä.

2. *Systemfehler beeinflussende Körper- und Umgebungsfaktoren*: Obwohl den oben genannten Leistungskenndaten eine gewisse Generalisierbarkeit zugeschrieben wird, die verschiedene Systeme vergleichbar machen soll, wird in der Regel gleichzeitig konstatiert, dass sie stark anwendungsabhängig sind. So mögen mit Menschen im Alter von 20 bis 40 Jahren getestete Fingerabdruckerkennungssysteme ganz andere Performanzraten aufweisen als dieselben Systeme, die mit Menschen zwischen 40 und 80 Jahren getestet wurden. Das Alter der betroffenen Personen wäre in diesem Fall ein problematischer Faktor für die Funktionstüchtigkeit des Systems. Es ist eine Fehlerursache, die im schlechtesten Fall allerdings als äußerer, das System störender Fehler gewertet wird.

3. *Überwindungsfehler und Störanfälligkeit*: Fehler, die durch Manipulationen des Systems oder unerwartete Störungen entstehen können. Insbesondere für ersteren Fall gibt es ein typisches Vokabular, von dem erste wichtige Begriffe hier kurz angeführt seien:[219]

[218] Siehe hierzu *Abschnitt: Erkennungs- und Vergleichsfehlerraten* (S. 97).

[219] Die Begriffe werden auch allgemein so in der IT-Sicherheit genutzt. Die Auswahl und die sinngemäß wiedergegebenen Definitionen stammen aus Maltoni u. a. 2009, S. 50 sowie Dunstone und Yager 2009, S. 73. Ein breiterer Überblick über das Gebiet findet sich in *Kapitel 3.4 Überwindungsfehler* (S. 111).

- *Spoof Attack*: Versuch einer Person, sich durch Täuschung als jemand anderes auszugeben und dadurch das System zu überlisten,
- *Vulnerability*: mögliche potentielle Sicherheitslücke für eine Schädigung der Funktionstüchtigkeit eines biometrischen Systems,
- *Denial-of Service*: absichtliche böswillige Lahmlegung der Funktionstüchtigkeit des Systems,
- *Circumvention/Intrusion*: unerlaubte Nutzung oder Manipulation des Systems durch einen nicht autorisierten Nutzer,
- *Function Creep*: Verwendung biometrischer Daten für einen anderen als den intendierten Zweck,
- *Repudiation*: Abstreiten der Systemnutzung seitens eines autorisierten Nutzers.

4. *Begriffsfehler*: Erkenntnistheoretische Kategorienfehler und Missverständnisse, die durch mehrdeutige und in der Biometrie metaphorisch genutzte Begriffe entstehen, die im Alltag oder anderen Disziplinen andere Bedeutungen haben. Hierzu gehören beispielsweise Begriffe wie *Identität* oder auch das militärische Vokabular aus dem Gebiet der Überwindungsfehler.

5. *Gesellschaftliche Fehler*: Fehler, die sich aus der politischen Anwendung der biometrischen Systeme ergeben; beispielsweise können sie als Sicherheitstechniken zu Fehlern in der korrekten Auslegung der Grundrechte führen; falsche Annahmen über Sicherheitsbedürfnisse oder Kriminalitätsraten können der Berechnung der Fehlerwahrscheinlichkeiten zugrunde liegen – teilweise sind dies auch normative Fehler, die allerdings nicht so stark formalisiert sind wie Systemfehler. Auch wirtschaftspolitische Fehlentscheidungen gehören dazu: zum Beispiel falsche Einsparungen oder Investitionen bei der Entwicklung eines Biometrie-Produkts oder Fehleinschätzungen der volkswirtschaftlichen Bedeutung der Biometrie-Industrie.

2.6 Resümee

Im Zentrum dieser Arbeit stehen die Fehler von Systemen, die genau eines ganz besonders verhindern sollen: Fehler bei der Wiedererkennung von Menschen durch andere Menschen. In den letzten Abschnitten wurde skizziert, wie dieses Anliegen in der Biometrie mit den Werkzeugen der Signalverarbeitung und Mustererkennung angegangen wird und welcher Begriffsapparat innerhalb der Biometrie inzwischen kanonisiert wurde, um adäquate eindeutige Problembeschreibungen zu ermöglichen.

James L. Wayman, der seit den 1990ern u. a. maßgebliche Arbeiten zur Systematisierung der Biometrie als informatisches Forschungsfeld publiziert hat, konstatierte auf

der *Biometrics Consortium Conference* (BCC) im Jahr 2013,[220] das er als 50. Geburtstag der automatisierten Personenerkennung bezeichnete, einen bedeutsamen Paradigmenwechsel in der Biometrie. Dieser sei angeführt von der ISO/IEC und der amerikanischen *National Academy of Sciences* (NAS). Im Selbstverständnis der Biometrie würden sich allmählich Konzepte aus Philosophie und anderen Wissenschaften niederschlagen. Biometrie müsse als Mensch-Maschine-Schnittstelle und nicht als Technologie gesehen werden, was sich in Performanzmessungen zeige, in der konkrete Menschen in ihrer Umwelt und die Technik zusammen berücksichtigt werden.[221] Eine Rückkopplung an die Terminologie bleibt hierbei nicht aus – das Ziel der normativen Begriffsdebatten im Rahmen der Glossare und Taxonomien sei „Monosemy", verstanden als „One-to-one mapping of terms and concepts".[222]

Die Begrifflichkeiten der Biometrie, ja selbst die Beschreibung des eigentlichen Problems, das die Biometrie lösen soll, unterliegen also noch einer großen Dynamik. Der bisher gegebene Überblick über das Gebiet der informatischen Biometrie ist Ausgangsbasis als auch Gegenstand einer Detailkritik der vielen vermeintlich fest definierten oder gar selbstevidenten Konzepte automatischer Personenwiedererkennung, die nicht allein auf technischer, sondern auch auf ökonomischer, philosophischer, politischer und sozialer Ebene äußerst fragil sind.

[220] Diese Konferenz fand seit 1992 bis 2014 mindestens einmal jährlich in den USA statt. Sie war Austauschplattform für Industrie und staatliche Organisationen mit Interessen in diesem Bereich. Getragen wurde der Zusammenschluss organisatorisch von Vertreterinnen der *National Security Agency* (NSA), NIST und der staatlich finanzierten Forschungsorganisation MITRE.

[221] Vgl. Wayman 2013, S. 41.

[222] Ebd.

3 Forschungsstand: Fehler von Fingerabdruckerkennungssystemen

Der Fehlerbegriff dieser Arbeit ist, wie in *Kapitel 2.5 Fehlerbegriffe* (S. 72) dargestellt, ein dynamisches Konzept. Es umfasst sowohl kalkulierte und teilweise formalisierbare Dysfunktionalitäten und Messfehler, die Abwägung widersprüchlicher Anforderungen an ein anwendungskonformes Design als auch die prinzipielle Kritik der gesellschaftlichen Rolle von Biometrie-Systemen. Innerhalb der Fehlerforschung kommt den Ingenieurwissenschaften, insbesondere der Informatik, eine wichtige Rolle zu.

Martin Weingardt, der 2004 die schon zitierte umfangreiche Forschungsarbeit zum Umgang mit Fehlern in Schule und Arbeitswelt vorgelegt hat, vergleicht darin vorhandene begriffliche Fehlersystematiken. Er konstatiert, dass die Informatik im weiteren Sinne der „Automatisierungstechnik" neben der Organisations- und Unternehmensberatung und der Evolutionsbiologie eine zentrale Rolle innerhalb einer Fehlerforschung spiele. Neu sei dort gewesen, dass der Fehler vom menschlichen Handeln entkoppelt betrachtet und somit ein systemischer Fehlerbegriff entwickelt wurde.[223] Das System kann hierbei ein technisches, elektronisches, organisatorisches oder natürliches sein und hat einen „eigenständigen Umgang mit als ‚Fehler' bezeichneten Ereignissen".[224]

Tatsächlich ist die Fehlerforschung in der Informatik ein bedeutsamer Zweig. Die Computergeschichte ist auch eine Geschichte fataler Softwarefehler, die die Entwicklung standardisierter Methoden der Spezifikation, Verifikation und des Testens von Software nach sich ziehen musste.[225] Schlingloff, der zur Qualitätssicherung von Software forscht, hält „hunderprozentig korrekte Programme", auch wenn sie selten in der Realität vorkommen, für möglich.[226] Im *Reliability Engineering* wird die Frage nach einer absoluten Fehlerfreiheit und Störungssicherheit eines Systems aber weder mit Ja noch mit Nein beantwortet, sondern, so Birloni, es sei möglich, für einen gegebenen Zeitraum eine Wahrscheinlichkeit für die Ausfallsicherheit anzugeben.[227]

Viele Softwarefehler sind letztlich Resultate von Konstruktionskompromissen mit am Ende schwerwiegenden Folgen, wie Coy historisch mit Verweis auf Speicherüberlauffehler und Rechenfehler durch Gleitkommaarithmetik zeigt.[228]

---

[223] Vgl. Weingardt 2004, S. 226 f.

[224] Ebd., S. 227.

[225] Vgl. Schlingloff 2006. Im Aufsatz wird eine Reihe berühmter Softwarefehler besprochen.

[226] Ebd., S. 329.

[227] Vgl. Birolini 2004, S. 1.

[228] Vgl. Coy 2009.

> „Ziel verantwortungsbewusster Technik ist es, denkbare Anfangsfehler auszuschließen oder in ihren Wirkungen zu begrenzen. So rechnen moderne Programmiersprachen mit Ausnahmefehlern (*exceptions*), die etwa durch Hardwarefehler oder durch unbedachte Programmierung (z. B. Division durch Null, Größenüberlauf) entstehen können und lassen eine Fehlerbehandlung (*exception handling*) zu, bevor der Prozessor in einen unkontrollierten Zustand gerät. Nur: Die Ausnahme muss vorher gedacht werden."[229]

Wichtig für ein Lernen aus Fehlern in der Softwaretechnik sind offene Standards, die, wie Coy ebenfalls feststellt, eine leichtere Erkennung von Fehlern ermöglichen, da sich die Systeme dann gleich verhalten.[230] Auch in der Biometrie ist man darum bemüht, Industriestandards zu schaffen, die durch die offiziellen internationalen Normungsinstitutionen akkreditiert sind – wirklich zugänglich sind die teuren Normendokumente allerdings nur für größere Firmen. Dennoch sind sie auch in dieser Arbeit ein wichtiger Ankerpunkt für schon erreichte Kompromisse im Rahmen eines verbindlichen, aber nicht zwangsläufig verlässlichen Biometriesystem-Designs. Von welchen Kompromissen dieses Design speziell geprägt ist und wie sich die Fehlerkategorien dieser Untersuchung daraus ergeben, wird im folgenden *Kapitel 3.1 Fehler und Biometriesystem-Design* genauer erläutert. In den daran anschließenden Kapiteln, die diese Kategorien in große Gruppen zusammenfassen – quantifizierte/formalisierte Fehler (3.2), unpassende Umgebung/unpassender Mensch (3.3), Überwindungsfehler (3.4), vieldeutige Grundbegriffe (3.5), Fehler im gesellschaftlichen Kontext (3.6) –, werden die in der Fachliteratur zu findenden Einteilungen entsprechend zugeordnet und diskutiert.

Die Forschung zu diesem Thema, ja selbst zum Oberthema der Fingerabdruckerkennung ist disparat, auch aus der Innenperspektive der informatischen Biometriker. Davide Maltoni, Dario Maio, Anil K. Jain und Salil Prabhakar konstatierten zur Veröffentlichung der zweiten Auflage des »Handbook of Fingerprint Recognition«:

> „Over 500 papers on fingerprint recognition were published in the last 5 years (2003 to 2008) alone! Fingerprint recognition literature is sometimes chaotic and, due to different (and often cumbersome) notations and conventions followed in the literature, it is not easy to understand the differences among the plethora of published algorithms."[231]

Auch in den darauf folgenden fünf Jahren, zwischen 2009 und 2014, sind weit mehr als 500 englischsprachige Veröffentlichungen, die die Implementierung automatisierter

---

[229] Coy 2009, S. 332.

[230] Vgl. ebd., S. 351.

[231] Maltoni u. a. 2009, S. xiii-xiv. Später im Text geben die Autoren eine Grafik zur wachsenden Anzahl der in den letzten 30 Jahren publizierten wissenschaftlichen Texte im Bereich der Forschung zur automatischen Fingerabdruckerkennung an, ohne Angabe oder Hinweis auf ihre Quellen. Demnach gab es in den 1980er Jahren lediglich eine Handvoll solcher Publikationen. Mit etwa zwei Dutzend Texten zum Thema ließ sich Ende der 1990er Jahre ein leichter Anstieg verzeichnen. Ab 2004 erschienen schließlich bereits mehr als 100 Artikel pro Jahr. (vgl. ebd., S. 55).

Fingerabdruckerkennung betreffen, in einschlägigen Fachjournalen und Konferenzbänden erschienen.[232] In den großen Datenbanken für wissenschaftliche Texte wie SCOPUS oder *Web of Science* gibt es in den Natur- und Technikwissenschaften für die Suche nach den Schlagworten ‚*fingerprint* AND *biometrics*' für die letzten fünf Jahre jeweils zwischen 1300 und 1600 Treffer, davon ist etwa, angesichts der Titel und Abstracts, ein gutes Drittel tatsächlich mit biometrischer Fingerbilderkennungstechnik befasst.

Im Vordergrund der technischen Literatur stehen in Bezug auf das Fehlermanagement die Themen Qualitätszertifizierung von Aufnahmegeräten, Leistungsfähigkeit und Korrektheit von Fingerabdruckerkennungsalgorithmen, einzelner Systemkomponenten sowie des technischen Gesamtsystems.[233] Außerdem spielt das *Security Engineering*, insbesondere die *Liveness Detection*, eine zentrale Rolle. Auch wenn es vereinzelte Artikel mit inter- oder transdisziplinärem Charakter gibt, sind Fragen der Gebrauchstauglichkeit von Mensch-Maschine-Schnittstellen-Problemen jenseits von *Security Engineering* und Akzeptanzsteigerung kaum ein Thema. Die Vermittlung biometrischer Fehler an betroffene Personen oder gar konkrete Lehr- und Lernstrategien für deren Aufklärung werden so gut wie nicht thematisiert. Einige der Fachbücher aus dem deutsch- oder englischsprachigen Bereich verstehen sich zwar auch als Nachschlagewerke für Studierende in Hochschulkursen, sind aber nicht didaktisch aufbereitet.

Hierzu gehört an allererster Stelle das weitestgehend monographische und schon mehrfach herangezogene Überblickswerk »Handbook of Fingerprint Recognition«, das zuerst 2003 und 2009 in zweiter Auflage erschienen ist. Es bietet eine umfassende Synthese der vielfältigen technischen Entwicklungen des Gebiets. Die Autoren thematisieren innerhalb ihres Buches im Rahmen der Einleitung Systemfehler nur auf wenigen Seiten. Das sind die bei Performanzmessungen erfassten Fehlerraten (hier in *Unterkapitel 3.2.2 Systemfehler und Performanzmetrik* vorgestellt). *Usability* wird weniger in Hinblick auf Gebrauchstauglichkeit für die betroffenen Personen denn auf Datensicherheit thematisiert, worunter dann auch vermittelt Datenschutz fällt. Es geht hierbei

---

[232] Dazu gehören die Journale *Pattern Recognition* und *Pattern Recognition Letters* sowie die jährlichen Konferenzbände der *International Conference on Biometrics* der *International Association for Pattern Recognition*, die Konferenzbände der *Biometrics Special Interest Group* (BIOSIG) der Gesellschaft für Informatik und der *Computer Society Conference on Computer Vision and Pattern Recognition* des *Institute of Electrical and Electronics Engineers* (IEEE) sowie der jährlichen Konferenz *Biometrics: Theory, Applications and Systems* des *Biometrics Council* und der IEEE-Gruppe *Systems, Man, and Cybernetics Society*, die Journale *Transactions on Pattern Analysis and Machine Intelligence* und *Transactions on Information Forensics and Security* der IEEE. Daneben gibt es sehr viele weitere Veröffentlichungen in diversen Journalen aus Forensik, Elektrotechnik, Künstlicher Intelligenz, Biotechnologie, Telekommunikation oder Optik-Journalen.

[233] Vgl. Ferrara 2010, S. 1 Der Autor nennt sie „some of the main problems of fingerprint-based biometric systems" (ebd., S. 1 f.).

in der Regel vor allem um die Wahrung der ökonomischen Interessen der Betreiber, sofern diese wichtige Kunden in kommerziellen Anwendungen darstellen. In einem eigenen Kapitel zur »Individuality of Fingerprints« wird die Problematik der grundlegenden Infragestellung des Fingerabdrucks als wissenschaftlich fundiertes Beweismittel in Strafverfahren, wie sie in den 1990er Jahren begann, eingehend auf stochastischer Ebene thematisiert. Hier ist bemerkenswert, dass einer ausführlichen wissenschaftlichen Replik auf eine rechts- und erkenntnistheoretische sowie historische Hauptkritik an den Prämissen der Fingerabdruckerkennung viel Platz eingeräumt wird. In anderen Grundlagenbüchern der informatischen Biometrie wird sie sonst gar nicht oder nur nebenbei abgehandelt. Des Weiteren ist eines der neun Kapitel des Buches dem Problembereich »Securing Biometric Systems« gewidmet.

Eine erhebliche Bedeutung in der Performanz- und Sicherheitsforschung haben die großen, unregelmäßig stattfindenden internationalen Wettbewerbe, die Benchmarks der aktuellen Systeme erstellen. Dazu gehören die Wettbwerbe *Fingerprint Verification Competition* (FVC),[234] ausgerichtet vom BioLab in Bologna, das eine führende Rolle in der anglo-amerikanischen und europäischen Biometrie-Forschung spielt, die *Liveness Detection Competition* (LivDet) oder die *Fingerprint Vendor Technology Evaluation* (FpVTE) des amerikanischen *National Institute of Standards and Technology* (NIST).

Wichtige internationale Referenzen für Mindestanforderungen, die hoheitliche Biometrie-Produkte erfüllen müssen, bilden die Vorgaben für maschinell lesbare Reisedokumente der *International Civil Aviation Organization* (ICAO)[235] sowie die umfangreichen Normen der ISO/IEC.[236] Zu den wichtigsten Blaupausen hierfür gehörten hier die am weitesten entwickelten Standards in den USA. Diese wurden anfangs vor allem im kriminaltechnischen Bereich durch das FBI zusammen mit der staatlichen Normbehörde NIST sowie das private *American National Standards Institute* (ANSI) vorangetrieben. Die Standards und Empfehlungen in Deutschland und Europa werden in Einklang mit denen des Subcommittee 37 »Biometrics« (im ISO/IEC JTC 1) entwickelt.[237]

Der Forschungsstand wird entlang der oben aufgeführten Problembereiche in den folgenden Kapiteln vertieft, innerhalb derer Dysfunktionalitäten, widersprüchliche Anforderungen an ein anwendungskonformes Design, prinzipielle Infragestellung von oder Kritik an Biometrie-Systemen auf sehr verschiedene Weise thematisiert werden. Neben den bereits angeführten Quellen werden auch Artikel aus Konferenzpublikationen und wissenschaftlichen Journalen sowie industrielle Whitepapers herangezogen.

---

[234] Vgl. Cappelli, Ferrara, Franco u. a. 2007, Cappelli und Maltoni 2010.

[235] Vgl. ICAO Doc 9303 2008b.

[236] Die inzwischen weit mehr als 100 Dokumente umfassenden biometrie-relevanten Standards stammen von den ISO/IEC-Untergliederungen Subcommittee (SC) 17 »Cards and Personal Identification«, SC 27 »IT Security techniques« und SC 37 »Biometrics«.

[237] Zur Struktur des SC37 sowie den Spiegelgremien siehe auch *Unterkapitel 4.3.3 Normung und Harmonisierung* (S. 164).

Der Schwerpunkt liegt dabei zwar auf Veröffentlichungen der Informatik. Texte aus transdisziplinären Kooperationen zwischen Informatik und anderen Gebieten, insbesondere sozial- und rechtswissenschaftliche sowie philosophische Analysen, werden aber zusätzlich herangezogen, da sie bestimmte Ideen und Zwecke der Biometrie auf grundlegende Weise in Frage stellen.

Ein besonderer Teil am Ende ist das *Kapitel 3.7 Bildungsprojekte zur Biometrie und die Rolle der Fehler* (S. 124), in dem knapp skizziert wird, wie die institutionalisierte Ausbildung im Fachgebiet der Biometrie sich derzeit gestaltet, welche didaktischen Leitmotive vorherrschen und welche Rolle Fehler dabei spielen.

3.1 Fehler und Biometriesystem-Design

Innerhalb der Softwareentwicklung und des *Systems Design* wird nach Modellen gesucht, möglichst viele auch schlecht zu formalisierende Problemstellungen derart handhabbar abzubilden, dass man ein spezifisches (Software-)System als dynamische Lösung entwerfen kann. Für Entwurf und Gestaltung – Design – eines Biometrie-Systems gibt es demnach gestalterische Anforderungen und an typischen Entwurfsmodellen orientierte Strukturen, die dazu dienen, viele bekannte Fehler und Probleme, die häufig einander bedingen, sinnvoll mit- und gegeneinander auszubalancieren. Aus Sicht der Software- und Hardwareentwicklung wird dies positiv formuliert: Jeder Design-Prozess hat die Entwicklung eines Systems zum Ziel, das den konkreten Anforderungen der gewünschten Anwendung genügt.[238] Insofern ist das Design grundsätzlich eine Problemlösung, bei der viele kleine Teilprobleme gelöst oder zumindest von den Anwenderinnen[239] besser akzeptierten Kompromisslösungen zugeführt werden.

Ruud Bolle, Jonathan Connell, Sharath Pankanti, Nalini Ratha und Andrew Senior sehen den Entwurf eines Biometrie-Systems als ein kompliziertes Puzzle:

> „Most importantly, a biometric authentication system has to guarantee security, which implies accuracy, without compromising too much on the convenience of its users, *and* it has to do this cost effectively.“[240]

Anders gesagt sind ein anforderungsgerechter Entwurf, dessen Implementierung sowie die Instandhaltung eines Biometrie-Systems insgesamt ein komplexes praktisches Problem, bei dem die Berücksichtigung quantifizierter Fehler nur einen Bruchteil der Lösung darstellt.

---

[238] Vgl. Jain und Nandakumar 2009, S. 136.

[239] In diesem Falle sind mit Anwendern vor allem bspw. staatliche Exekutivorgane (Grenzkontrollen), Arbeitgeber (beschränkter Zugang zu Räumen) oder Verkäufer (Bezahlung im Supermarkt) gemeint. Der Begriff des Anwenders ist in der Biometrie weit gefächert – siehe hierzu *Unterkapitel 4.3.1 User und Usees* (S. 152).

[240] Bolle u. a. 2004, S. 10 f., kursiv im Orig.

In Einklang zu bringen sind folgende Faktoren: die Erkennungsgenauigkeit des Systems (*System Accuracy*), seine Rechengeschwindigkeit (*Computational Speed*), die Form des Umgangs mit unerwarteten Situationen (*Exception Handling*), die Systemkosten (*System Cost*) sowie Sicherheit (*Security*) und Datenschutzregeln (*Privacy*).[241] Diese Faktoren werden von Jain und Nandakumar etwas verändert adaptiert. Statt von Rechengeschwindigkeit wird von (Daten-)Durchsatz (*Throughput*) gesprochen und die Behandlungen von Ausnahmesituationen werden unter den Begriff der Gebrauchstauglichkeit (*Usability*) gefasst.[242] Derartige Situationen entständen durch unerfahrene, die Interaktion mit dem System meidende, die geprüften Charakteristika nicht besitzende oder einfach einen ‚schlechten biometrischen Tag' habende Nutzerinnen.[243] Der Begriff der Usability meint aber mehr. Zu ihm gehören *Effectiveness* („Können Nutzerinnen erfolgreich ein hochqualitatives Sample zur Verfügung stellen?"), *Efficiency* („Können Nutzerinnen sich schnell ohne Fehler authentifizieren?"), *Satisfaction* („Fühlen Nutzerinnen sich bei der Benutzung des Systems wohl?") und *Learnability* („Gewöhnen sich die Nutzerinnen an das System?").[244]

Maltoni, Jain und Prabhakar sowie Dunstone und Yager schlagen ähnliche Kriterien vor, die auch die Wahl einer geeigneten Charakteristik vorgeben. Erstere unterscheiden dabei zwischen Anforderungen an die „anatomische oder verhaltensbezogene Charakteristik" – *Universality* (bei Dunstone/Yager: *Inclusiveness*), *Distinctiveness*, *Permanence* (bei Dunstone/Yager: *Stability*), *Collectability* (fällt bei Dunstone/Yager unter *Inclusiveness*)[245] – und Aspekten, die im praktischen Einsatz berücksichtigt werden müssten – *Performance*, *Acceptability* und *Circumvention*.[246] *Performance* umfasst hier die Erkennungsgenauigkeit, die Rechengeschwindigkeit, den Ressourcenverbrauch und die Beständigkeit gegenüber operationalen und umweltbedingten Faktoren. Bis auf die Performanz integrieren Dunstone und Yager dagegen alle diese Faktoren als „biometrische Attribute" und fächern diese noch breiter auf.[247] So gehören dazu noch weitere Kriterien wie *Scalability* für die effiziente Verarbeitung biometrischer Daten, *Insensitivity* für die Unempfindlichkeit des Systems gegenüber Umwelteinflüssen wie bspw. Licht und Temperatur, *Maintenance* für die Abnutzungsbeständigkeit der Systemsensorik sowie *Quality* für die Fähigkeit des Systems, Samples in hoher Qualität zu akquirieren. Der Grad der Überwindungsmöglichkeiten des Systems (*Circumvention*) wird bei Dunstone und Yager unter den Begriff der *Vulnerability* oder an anderer

[241] Vgl. Bolle u. a. 2004, S. 9 ff.

[242] Vgl. Jain und Nandakumar 2009, S. 137.

[243] Vgl. Bolle u. a. 2004, S. 9. Anführungszeichen im Orig., von Verfasserin übersetzt.

[244] Jain und Nandakumar 2009, S. 137, Fragen von Verfasserin übersetzt.

[245] Zur Bedeutung dieser Eigenschaften siehe *Unterkapitel 2.2.2 Eindeutigkeit, Permanenz, Universalität, Messbarkeit, Akzeptanz* (S. 34).

[246] Vgl. Maltoni u. a. 2009, S. 8 ff.

[247] Vgl. Dunstone und Yager 2009, S. 12 f.

Stelle *Resistance to Circumvention* subsumiert. Außerdem wird das Kriterium für die Möglichkeit der Integration des Biometrie-Systems mit anderen Authentifizierungsmechanismen wie Passwörtern oder Chipkarten als *Integration* erwähnt.

Statt *Acceptability*, das allgemein das Einverstandensein der Nutzerinnen mit der Nutzung eines biometrischen Identifikators im Alltag ist, werden bei Dunstone und Yager die Kriterien *Usability*, *Health* und *Privacy* als Anforderungen im Sinne der Eigentümerinnen einer biometrischen Eigenschaft beschrieben. Diesen dürfe kein gesundheitlicher Schaden beim biometrischen Erkennen entstehen, und im besten Falle sollten sie die biometrische Erfassung im Vorfeld gestatten. *Usability* beschreiben Dunstone und Yager wie folgt:

> „A major selling feature in the adoption of biometrics is convenience. If a biometric is difficult or slow to use, it probably won't be adopted. Ideally, the ergonomics of the sensor will make it so simple to use that the authentication will barely be noticed. Usability is an especially important factor for people with disabilities (e.g. people who are vision or mobility impaired). This is particularly crucial in places where a biometric will be used frequently, such as for access control. Although, in some cases, mainly where a biometric is used for surveillance, this may not be relevant."[248]

Diese Art von *Convenience* ist schließlich eines der Kriterien, die in die Systemkosten einfließen, die ein weiteres „biometrisches Attribut" bei Dunstone/Yager sind. Wirtschaftlichkeitsfaktoren seien zudem „enhanced security, reduced cost for employing human operators or reduced cost from token loss."[249]

Biometrische Typen, womit sie Charakteristika wie Hände, Finger, Gesicht, Iris usw. meinen, hätten jeweils spezifische Stärken hinsichtlich der Ausprägung der einzelnen Attribute. Da allerdings die Wichtigkeit jedes einzelnen Attributs je nach Anwendungskontext variiere, wie in Tabelle 3.1 dargestellt, lässt sich das geeignete biometrische Charakteristikum (oder mehrere) entlang seiner Stärken für den jeweils relevanten Kontext heraussuchen. Eine dafür geeignete Tabelle bieten wiederum Maltoni et al. an (Tabelle 3.2). Die qualitativen Gewichtungen „niedrige", „mittlere" oder „hohe" Relevanz/Sicherheit sind in beiden Publikationen nicht empirisch belegt, sondern zu illustrativen Zwecken gedacht bzw. nach der persönlichen Wahrnehmung der Autoren zugeordnet.[250] Obwohl die Entscheidungsmetriken bereits stark vereinfacht sind, wird die Komplexität der sinnvollen Einschätzung deutlich, welche Eigenschaften eines biometrischen Merkmals wie relevant oder irrelevant in einem sehr grob vereinfachten Anwendungskontext sind (Laptop-Sensor, Ausweisvergabe, verdeckte Ermittlung). Es handelt sich hier insgesamt um ein Design-Problem, das bei jeder einzelnen Anwendung eine eigene Lösungsstrategie erfordert.

[248] Ebd., S. 12.

[249] Ebd., S. 13.

[250] Vgl. Ebd. bzw. Maltoni u. a. 2009, S. 11.

Biometric Attribute	(a) Laptop Sensor	(b) Passport Issuing	(c) Covert Surveillance
Distinctiveness	High	High	High
Stability	Med	High	High
Scalability	Low	High	High
Usability	High	Med	-
Inclusiveness	Med	High	High
Insensitivity	High	High	Med
Vulnerability	High	High	Med
Privacy	Med	High	High
Maintenance	High	High	Low
Health	High	High	-
Quality	High	High	High
Integration	Med	High	Low
Cost Sensitivity	High	Low	Med

Tabelle 3.1: Vergleich der Wichtigkeit typischer Anforderungskategorien an ein Biometrie-System für drei verschiedene Anwendungsbereiche. Tabelle aus Dunstone und Yager 2009, S. 13, © Springer-Verlag.

Biometric identifier	**Universilaty**	**Distinctivness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Hand/finger vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Tabelle 3.2: Vergleich der Ausprägung bestimmter Eigenschaften biometrischer Charakteristika (H: High, M: Medium, L: Low). Tabelle aus Maltoni u. a. 2009, S. 11, © Springer-Verlag. Eine Tabelle gleicher Struktur, ohne „Keystroke“ und, außer bei „Fingerprint”, mit teilweise anderen Werten, findet sich in Jain, Ross und Pankanti 2006, S. 127.

Auf weitere Ansätze, Rahmenwerke für eine erfolgreiche Biometriesystem-Entwicklung zu entwickeln, verweist ein Abschlussbericht des EU-Forschungsprojekts »BIOVISION – Roadmap to Successful Deployments from the User and System Integrator Perspective«.[251] Interessant ist hier unter anderem auch die Idee der *Biometric and Token Technology Application Modeling Language* (BANTAM) von Julian Ashbourn, die er – offensichtlich wie so einige in der Biometrie-Entwickler-Community eher als Einzelkämpfer – bereits seit Anfang der nuller Jahre verfolgt, die aber leider nur für das Windows-Betriebssystem implementiert ist. Sie soll auch als Lernsoftware gedacht sein, wird aber lediglich durch das käuflich zu erwerbende Buch von Ashbourn dokumentiert und hat in der Fachliteratur bisher wenig Echo erfahren.[252]

Der Bericht selbst gibt ebenfalls Eckpunkte für erfolgreiche Markteinführung biometrischer Technik an. Zunächst werden vier zentrale Anwendungsfelder für Biometrie-Applikationen benannt: 1. Zugangskontrolle, 2. Transaktionssicherheit, 3. Nachverfolgung und Aufspüren und 4. Personalisierung.[253] Dann wird ein dreidimensionales „Application Pull Framework" angegeben, das die einen Biometrieeinsatz steuernden Eigenschaften in den Kategorien *Akteure des Markts*, *Anforderungen* und – eben schon genannt – *Anwendungsfelder* anordnet. Als Beispiele für Anforderungen an eine Biometrieanwendung aus Sicht eines Betreibers benennen die Autoren des Berichts *Performance* mit den Teilanforderungen *Security Class*, *Recognition Class*, *Enrolment Specific Performance* sowie *Environment* in den Abstufungen *Integration Environment*, *Physical Environment Conditions*, *End User Environment* und *Operator Environment*. Die Marktakteure werden nach *Sensor Manufacturer*, *Algorithm and Software Developer*, *Biometric System Integrator*, *System Provider* und *End User* klassifiziert.

Eine weitere Taxonomie für eine erleichterte Einschätzung der konkreten Einsatzumgebung eines biometrischen Systems, die vor allem die Rolle der betroffenen Personen im Verhältnis zum System, aber auch die Umgebungsbedingungen tangiert, gibt Wayman an:[254]

- *Overt*/*Covert* (auch: *Aware* bzw. *Cognizant*/*Unaware*): Ist sich die betroffene Person der Messung eines biometrischen Merkmals bewusst, ist die Benutzung *offenkundig*. Weiß sie davon nichts, erfolgt die Nutzung *verdeckt*. Letzteres ist im Fingerabdruckbereich auf mehrerlei Art möglich – zum Beispiel durch Reproduktion latenter Abdrücke auf Gläsern, durch Erfassung von Fingerkuppen mittels hochauflösender Kameras oder „Touch"-Sensoren wie in Smartphones.

[251] Vgl. Albrecht u. a. 2003, S. 74.

[252] Vgl. Ashbourn 2015 (1. Auflage 2003). BANTAM-Webseite: http://biometrics.bl.ee, letzter Abruf: 23.7.2017.

[253] Vgl. Albrecht u. a. 2003, S. 34, von Verfasserin übersetzt.

[254] Vgl. Wayman 2005, S. 7 ff.

- *Habituated*/*Non-habituated*: Die betroffene Person ist den Umgang mit dem System entweder *gewohnt* oder eben (noch) *nicht gewohnt*.
- *Attended*/*Non-attended* (manchmal auch *Supervised*/*Unsupervised*): Wenn es jemanden gibt, die die betroffene Person durch den Erfassungsprozess führt, handelt es sich um eine *betreute* Nutzung. Ein typisches Beispiel ist hier die erkennungsdienstliche Behandlung. Verifikationen an einem persönlichen Rechner sind dagegen meist *unbetreut*.
- *Standard*/*Non-standard*: In ersterem Fall sind die Umgebungstemperatur, Luftdruck und Lichtbedingungen beispielsweise in einer Standard-Indoor-Situation gut kontrollierbar und stabil. In letzterem handelt es sich um schwerer kontrollierbare Bedingungen, wie sie unter Umständen zum Beispiel außerhalb eines Hauses vorliegen.
- *Public*/*Private*: Ein biometrische Anwendung kann hoheitlich und *öffentlich* betrieben werden. Sie kann aber auch eine *privatwirtschaftliche* oder individuelle Anwendung sein. Wayman konstatiert hier einen Zusammenhang zur Kooperationsbereitschaft der betroffenen Personen.
- *Open*/*Closed*: Wenn das System mit anderen interagieren können soll, wie beispielsweise im Falle des Austauschs zwischen verschiedenen Ämtern oder der Nutzung zentraler Datenbanken durch verschiedene Einzelsysteme, ist es *offen*. Dann muss es standardisierte Speicher- und Austauschformate und Erfassungsmethoden geben. Für ein *geschlossenes* System können die Formate proprietär bleiben.

Weitere Begrifflichkeiten für Anwendungskontexte sind:[255]

- *On-line*/*Off-line*, wenn das System entweder unmittelbares, schnelles Feedback an die betroffene Person geben muss (Zugangskontrolle, System-Login) oder eine längere Antwortzeit und Hintergrundchecks möglich sind (Automatisiertes Fingerabdruckidentifizierungssystem (AFIS)).
- *Fully automatic*/*Semi-automatic*, wenn entweder das Enrolment durch die betroffene Person ohne anderes Personal selbständig mit einem Live-Scanner durchgeführt werden kann, es keine manuelle Qualitätskontrolle des Samples gibt und auch Merkmalsvergleich sowie Entscheidung automatisch ablaufen, oder wenn wie beim AFIS Papiervorlagen oder latente Fingerabdrücke eingescannt werden, Polizeibeamtinnen eine Verdächtige durch die erkennungsdienstliche Behandlung führen und Daktyloskopinnen vom AFIS gefundene Kandidatinnen nochmals manuell untersuchen.

[255] Vgl. Maltoni u. a. 2009, S. 6.

Neben Kriterien und Taxonomien wird der Design-Prozess häufig in bestimmte Phasen und Zyklen eingeteilt, in dem die bestmögliche Erfüllung aller genannten Anforderungen ausbalanciert wird, zum Beispiel wie folgt in drei Schritten:[256]

- Wahl der Architektur: Sollen die Templates zentral oder verteilt auf einer Server-Architektur (bei Identifikation zwingend), lokal bei der Nutzerin oder auf einem mobilen Gerät oder einer Smartcard gespeichert werden? Wo werden Template und gerade erfasstes Muster verglichen – Server, Client, mobil?

- Wahl der Hardware und Software: Ein biometrisches System wird in der Regel nicht von einem einzigen Unternehmen produziert. Einzelne Hard- und Softwarekomponenten verschiedener Firmen werden von einer Firma, die als Systemintegrator auftritt, als Gesamtsystem verkauft. So sind insbesondere Sensortechnik, Benutzerschnittstellen, Signalverarbeitungs- und Mustererkennungssoftware, Kommunikationskanäle, Datenbankdesign und interoperable Datenformate jeweils für sich sehr komplexe Komponenten, bei denen im Detail auf passende Anforderungskonformität geachtet werden muss.

- Festlegen von Administrationsrichtlinien (*Administration Policies*): Wie wird bei der Ersterfassung (Enrolment) abgesichert, dass niemand mit falscher Identität, zum Beispiel mittels gefälschten Ausweises oder gefälschter Geburtsurkunde gespeichert wird? Wie wird durch die Art und Weise der Ersterfassung gesichert, dass die bestmöglichen Samples verarbeitet werden (z. B. User-Training, alternativer Umgang mit Personen, bei denen ein biometrisches Merkmal nicht erfassbar ist)? Welche Konfiguration hat das System in Bezug auf die Schwelle, ab der zwei Muster als ausreichend ähnlich gewertet werden, um sie als von derselben Person stammend einzustufen, oder in Bezug auf die Anzahl der Vergleichsversuche bis zu einer Sperrung eines Accounts? Welche Konfiguration hat es in Bezug darauf, ab wann ein Template-Update notwendig ist? Welche Regeln erleichtern den Umgang mit dem System so, dass es für die „Datensubjekte“ nicht unangenehm ist, sich zu registrieren, selbst bei Verletzungen und ähnlichem, dass gleichzeitig aber damit verbundene Ausnahmerichtlinien nicht als Mittel zur Umgehung des Systems genutzt werden? Welche Kontrollmaßnahmen können etabliert werden, um die Templates zu schützen (z. B. durch regelmäßige Kontrolle der Protokolldateien der Template-Datenbank)?

Die Interpretationsspielräume und Wechselwirkungen zwischen den zahlreichen Anforderungen, denen Architektur, Hardware/Software und Richtlinien unterliegen, sind nicht nur zentral für einen adäquaten Entwurf eines Biometriesystems, sondern

[256] Die Schritte sind zusammengefasst von Jain und Nandakumar 2009, S. 138 f. übernommen.

auch für dessen realistische Repräsentation als ein anwendungsgebundener Kompromiss. Sämtliche aufgezählten Designkriterien sind Bereiche, in denen spezifische Fehler vermieden sollen. Sie subsumieren Fehlerkategorien, nach denen die folgenden Kapitel strukturiert sind:

1. Im *Kapitel 3.2 Quantifizierte oder stark formalisierte Fehlergrößen* werden die Kategorien Erkennungsgenauigkeit, Rechen- oder etwas weiter gefasst Verarbeitungsgeschwindigkeit und deren Skalierbarkeit, Normkonformität hinsichtlich interoperabler Daten- und Schnittstellenformate beschrieben.

   Dem Kapitel werden zum einen die gut mit Performanzmetriken abbildbaren Fehler von Fingerabdruckerkennungssystemen untergeordnet. Sie sind umfangreich erforscht, da sie allgemein innerhalb Signalverarbeitung und Mustererkennung geläufig sind. Zum anderen unterliegen biometrische Daten bestimmten Konformitätskriterien, zumindest, wenn es um interoperable Daten wie im hoheitlichen Bereich geht. Hier ergeben sich Fehler aus Abweichungen von den vorgegebenen Standards, die wiederum in Konformanztests festgestellt werden können. Auch diese sind mittels Standards formalisiert und vorgeschriebenen Überprüfungsmethoden unterworfen.

2. Wesentlich schwieriger formal zu fassen sind die die Performanz beeinflussenden Faktoren. Fingerbilderkennungssysteme müssen universal sein. Um zu gewährleisten, dass sie unabhängig von körperlichen Unterschieden (zum Beispiel schwitziger oder trockener, junger oder alter Haut) oder verschiedenen Umgebungsbedingungen immer gleich gut funktionieren, werden bestimmte körperliche sowie Umgebungsdispositionen und die Technik aufeinander abgestimmt. Im *Kapitel 3.3 Fehler durch dynamische Körper- und Umgebungsfaktoren* werden typische Klassifizierungen von Defiziten des Körpers, der Akzeptanz seitens der betroffenen Personen oder der Umgebungsbedingungen aus technischer Sicht aufgelistet, die sich umgekehrt auch als Defizite der Technik, sich an wandelnde Umgebungs-, Körperbedingungen und Nutzerinnenbedürfnisse anzupassen, lesen lassen.

   In Bezug auf das Systemdesign werden hier oben genannte Kriterien wie Unempfindlichkeit des Systems gegenüber Umwelteinflüssen wie bspw. Licht und Temperatur, Akzeptanz des Systems durch die betroffenen Personen, aber auch Fragen der *Usability* oder Gesundheitsverträglichkeit berührt. Auch die Fähigkeit des Systems, den für Biometrie tauglichen Körpermerkmalen zugeschriebenen Eigenschaften der Universalität, Eindeutigkeit und Beständigkeit auch wirklich gerecht zu werden, gehört zu den hier verhandelten möglichen Anpassungsfehlern.

3. In einer weiteren Perspektive – im *Kapitel 3.4 Überwindungsfehler* – stehen Fehler im Mittelpunkt, die im weiteren Sinne die Ablauf- und Ausfallsicherheit eines Fingerabdruckerkennungssystems (*Safety*) betreffen – hierzu gehören beispielsweise Regelungen für den Umgang mit unerwarteten Betriebsfehlern. Im engeren Sinne geht es hierbei um im Rahmen der Informationssicherheit (*Security*) einzuhaltende Schutzziele wie Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der verarbeiteten Daten. Hieran gekoppelt sind Überwindungsfehler im Bereich der IT-Sicherheit, die in der Regel auch – gerade auch in Bezug auf die konkreten Anforderungen an die Biometrie-Systeme – aus Sicht der Informatik kategorisiert werden. Andererseits fallen Fragen des Schutzes von betroffenen Personen, also des Datenschutzes, hierunter.

Schließlich folgen zwei weitere Fehlerkategorien, die sich nicht unmittelbar in den Attributen des Systemdesigns widerspiegeln, sondern grundsätzlicher Natur sind, weil sie sich mit erkenntnis- und begriffstheoretischen Voraussetzungen der Biometrie beschäftigen oder aber weil sie ein biometrisches System als Ganzes in einem konkreten gesellschaftlichen Kontext betrachten.

4. Ohne ganz grundlegende „wünschenswerte biometrische Attribute“[257] wie Permanenz, Eindeutigkeit und Universalität des Fingerabdrucks und ihren spezifischen Wert für die Personenerkennung hätte die biometrische Technik keinen Sinn. Im *Kapitel 3.5 Begriffs- und erkenntnistheoretische Probleme* werden prinzipielle Missverständnisse der Idee hinter der Technologie beleuchtet.

5. Mit allen oben genannten gehen auch Fehler- und Problemdiskussionen auf sozialer, juristischer, politischer, historischer, ökologischer, wirtschaftlicher oder künstlerischer Ebene einher. Im *Kapitel 3.6 Fehleruntersuchungen jenseits der Informatik* werden Sichten auf die biometrische Technik vorgestellt, die die Biometrie selbst als Fehler oder als einem gesellschaftlich problematischen Zweck dienend betrachten. Es geht hier um wissenschaftshistorische, soziale und politische Probleme der biometrischen Techniken, die im Design keine oder nur eine randständige Rolle spielen, und soll die Perspektive, die im *Kapitel 3.3 Fehler durch dynamische Körper- und Umgebungsfaktoren* eingenommen wird, wesentlich erweitern. Allerdings ist dieser Teil nur sehr knapp, auf eine Auswahl an Arbeiten beschränkt dargestellt, da er sonst den Rahmen der Arbeit sprengen würde.

[257] Dunstone/Yager beschreiben „desirable biometric attributes“ als „some general attributes that are desirable for good biometric operation“ (Dunstone und Yager 2009, S. 11), siehe auch Tabelle 3.1. Designanforderungen, die eher das Körpermerkmal betreffen, verschmelzen mit den Anforderungen an das für die entsprechende Ausprägung von Permanenz, Universalität oder Eindeutigkeit geeignete System.

3.2 Quantifizierte oder stark formalisierte Fehlergrößen

Quantitative Fehler- und Datendurchsatzraten biometrischer Systeme und ihrer einzelnen Komponenten werden bei technischen Performanzevaluationen erhoben. Sie sollen realitätsnahe und bezifferbare Prognosen über die Leistungsfähigkeit der Systeme bieten.[258] Es werden Fehler beim Mustervergleich, Fehler bei der sensorischen Erfassung des Merkmals sowie die Gesamtbearbeitungsgeschwindigkeit von Personen pro Zeiteinheit in Abhängigkeit von der Rechengeschwindigkeit und der Mensch-Maschine-Interaktion statistisch erfasst.

3.2.1 Performanzevaluationen

Die bekanntesten technischen Evaluationen für Fingerabdruckerkennungssysteme sind der *Fingerprint Verification Competition* (FVC) des *Biometric System Laboratory* der Universität Bologna, die *Fingerprint Vendor Technology Evaluation* (FpVTE), die *Minutiae Interoperability Exchange* (MINEX) sowie die *Slap Fingerprint Segmentation Evaluation* (SlapSeg) des NIST.[259] Modi nennt zudem den *Minutiae Template Interoperability Test* (MTIT) als einen wichtigen Interoperabilitätstest, bei dem auch Konformanz mit den in Dokument ISO/IEC 19794-2[260] vorgegebenen Kriterien für interoperable Minutiendatenformate getestet wurde. Dieser wurde im Rahmen des 6. Forschungsrahmenprogramms (*6th Framework Programmes for Research and Technological Development*, FP6) der Europäischen Kommission zwischen 2005 und 2007 unter der Leitung des britischen *National Physical Laboratory* (NPL) mit Beteiligung des Fraunhofer-Instituts für Sichere Informationstechnologie (Fraunhofer SIT) durchgeführt.[261]

Vor allem der FVC findet seit dem Jahr 2000 kontinuierlich statt. Bis 2006 gab es vier Einzelwettbewerbe (2000, 2002, 2004 und 2006). Seit 2009 läuft der Wettbewerb als ständig verfügbare „web-based automatic evaluation“ mit dem Titel *FVC-onGoing*.[262] Getestet werden verschiedene algorithmische Teilkomponenten eines Biometriesystems – inzwischen nicht mehr nur fingerabdruckbezogene. Dazu gehören Vergleichsfehlerraten bei einer Fingerbildverifikation mit Standardbildformaten, nach ISO-Formatvorgaben, Fingerbildverifikation verschlüsselter Templates, die Extraktion von *Orientation Images*, Fingerabdruckindizierung für AFIS, Handabdruckverifikation oder Konformanz von Gesichtsbildern mit ISO-Normen. Auf den zugehörigen Webseiten lassen sich detaillierte Performanzkenndaten für getestete Algorithmen anschauen.

[258] Vgl. ISO/IEC 19795-1:2006, S. vi.

[259] Vgl. Modi 2011, S. 48 ff.

[260] Siehe ISO/IEC 19794-2:2011.

[261] Vgl. CORDIS 2008b.

[262] Vgl. Dorizzi u. a. 2009, S. 726. Webseite: https://biolab.csr.unibo.it/FVCOnGoing, letzter Abruf: 22.7.2017.

Bevor in den folgenden Kapiteln auf die Vergleichsfehlerraten, die zu den besonders wichtigen Performanzkenndaten eines Biometriesystems gehören, näher eingegangen wird,[263] soll zunächst ein erster Eindruck von der Visualisierung der dort abrufbaren Testergebnisse gegeben werden. In Abbildung 3.1 werden zum einen die Verteilungen der Vergleichswerte (hier ingesamt als *Threshold* t bezeichnet) der Bilder identischer Finger (*Genuines*) und nicht-identischer Finger (*Impostors*) als diskrete Häufigkeitsverteilungen gezeigt. Die zugehörigen Fehlerraten, die unten näher erläutert werden, *False Match Rate* (FMR(t)) und *False Non-Match Rate* (FNMR(t)) werden zum anderen als Funktionsgraphen von t dargestellt. Außerdem werden *Detection-Error-Tradeoff* (DET)-Graphen genutzt (siehe Abbildung 3.2).

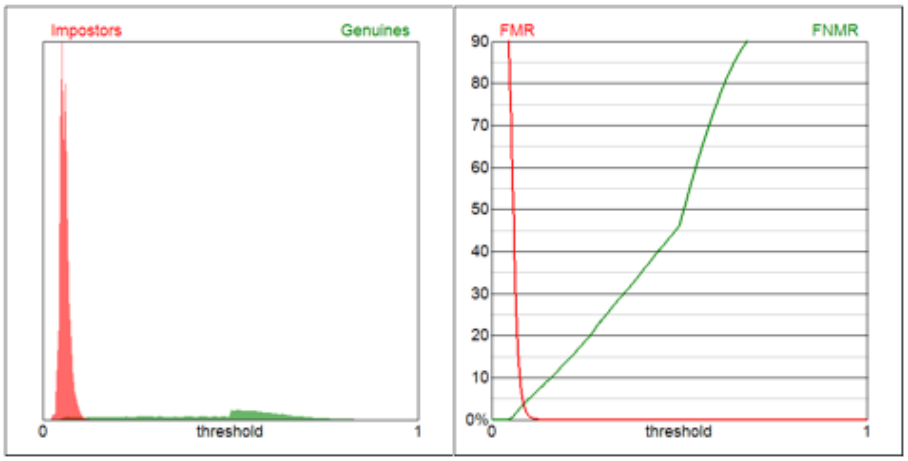


Abbildung 3.1: Der linke Graph zeigt die diskreten Verteilungen der Vergleichswerte (hier als Threshold t) für alle Vergleiche, der rechte die Fehlerraten FMR(t) und FNMR(t) des Vergleichsalgorithmus von SourceAFIS 1.1. Graphen vgl. Biometric System Laboratory 2010.

Performanztests wie der FVC haben wenig mit der Realität zu tun, da sie unter engen und kontrollierten Bedingungen stattfinden müssen, um statistisch valide Aussagen über die Leistungsfähigkeit eines Algorithmus treffen zu können. Diese Tests gehören zur Gruppe der sogenannten Technikevaluationen (*Technology Evaluation*). Schon hier gibt es ein erhebliches Grundproblem: die Beschaffung möglichst vieler realistischer Testdaten. Die Datenmengen sollten mindestens eine vierstellige Anzahl an Testsamples enthalten, um zu repräsentativen Ergebnissen zu kommen. Auch im Rahmen des Parameter-Tunings der Matcher und Extraktoren eines Biometrie-Systems bei Leistungstests sind große Datenmengen wünschenswert. Da deren Beschaffung sehr aufwendig ist, gibt es inzwischen eine *Synthetic Fingerprint Generation* (SFINGE):[264]

[263] Siehe *Abschnitt: Erkennungs- und Vergleichsfehlerraten* (S. 97).

[264] Das Kapitel »Synthetic Fingerprint Generation« in Maltoni u. a. 2009, S. 271–302, stammt von Raffaele Cappelli. Das zugehörige Software-Tool SFINGE wird vom *Biometric System Laboratory* der Universität Bologna angeboten, http://biolab.csr.unibo.it/sfinge.html, letzter Abruf: 22.7.2017.

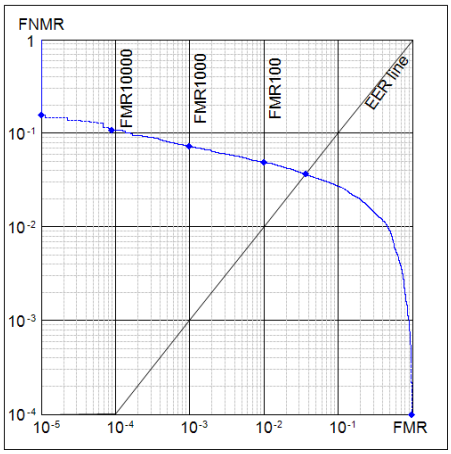


Abbildung 3.2: DET-Graph des SourceAFIS 1.1-Vergleichsalgorithmus. Graph vgl. Biometric System Laboratory 2010.

„The most desirable property of such a synthetic fingerprint generator is that it should be able to model the various inter-class and intra-class variations in fingerprint images observed in nature. In particular, multiple 'impressions' of the same 'virtual finger', should reflect:

- Different touching areas.
- Non-linear distortions produced by non-orthogonal pressure of the finger against the fingerprint scanner.
- Variations in the ridge line thickness given by pressure intensity or by skin dampness.
- Small cuts on the fingertip and other kinds of artifacts.
- Complex background such as those typically observed when the fingerprint scanner surface is dirty."[265]

Es ist so paradox wie erfindungsreich, die ja eigentlich natürliche Einzigartigkeit zu simulieren. Auch das Potential des Werkzeugs für gute Template-Fälschung ist sicherlich nicht uninteressant.

Gewissermaßen deutet sich hier auch eine höher gelagerte Problematik einer Fehlermessung im Labor an: das Mustererkennungsproblem wird komplett losgelöst von der realen Welt, für die es eigentlich gedacht ist.

Testumgebungen werden also nach Technik- (*Technology Evaluation*), Szenario- (*Scenario Evaluation*) und betrieblicher Erprobung (*Operational Evaluation*) unterschie-

[265] Maltoni u. a. 2009, S. 45.

den,[266] wobei dies grobe Abstufungen der Testkomplexität sind. Während eine Technikerprobung, wie geschildert, unter klar abgrenzbaren Laborbedingungen mit festen Testdatensätzen komponentenbezogen (vor allem Erfassung, Merkmalsextraktion und Vergleich) stattfindet und die Erhebung oben genannter Parameter kontrolliert möglich ist, ist eine Pilotstudie im Realbetrieb in der Regel nicht wiederholbar und objektivierbar. Zugleich aber können erst in einer operationalen Evaluation Datendurchsatzraten und Interaktionsdauern realistisch gemessen und unerwartete Fehler sowie komplexere qualitative Kategorien in die Beurteilung eines solchen Systems einbezogen werden.

Eine Szenarioevaluation ist zwischen beiden Testkontexten angesiedelt. Realweltliche Bedingungen werden simuliert. Die Abläufe sind allerdings noch stark gesteuert. Die Testpopulation wird gezielt zusammengestellt. Der Test ist bei guter Dokumentation der Umgebungsparameter wiederholbar. So muss beispielsweise festgehalten werden, ab wann ein Erfassungsversuch einer biometrischen Charakteristik als fehlgeschlagen gilt oder welche biometrischen Proben in die Berechnung der Fehlerraten einbezogen werden.

3.2.2 Systemfehler und Performanzmetrik

Für Performanzevaluationen gibt es im Allgemeinen inzwischen standardisierte, fest definierte Berechnungsformeln, Visualisierungs- und Testregeln in den Industrienormen, da es in der Fachliteratur keine einheitlichen methodischen Empfehlungen gibt.

Das *Subcommittee 37 »Biometrics«* (SC37) des JTC 1 der ISO/IEC als internationales, verschiedene Interessengruppen mit fachlicher Expertise versammelndes Gremium aggregiert im Bereich der Messung von Systemfehlern die breite Vielfalt sich widersprechender Testverfahren, selektiert daraus bewährte wissenschaftliche Methoden[267] und unterzieht diese regelmäßig einer Neuüberprüfung.[268] Die wichtigsten Dokumentreihen in diesem Zusammenhang sind:

- die Dokumentreihe »19795 – Information technology – Biometric performance testing and reporting« (bestehend aus derzeit sieben Dokumenten – hauptsächlich erstellt und gepflegt durch die *Working Group* 5 »Biometric testing and reporting«),

[266] In ISO/IEC 19795-1:2006, S. 38 werden die einzelnen Eigenschaften dieser Szenarien in einer Tabelle systematisch verglichen; hier erfolgt nur eine knappe Zusammenfassung.

[267] „The purpose of this part of ISO/lEC 19795 is to present the requirements and best scientific practices for conducting technical performance testing. This is necessary because even a short review of the technical literature on biometric device testing over the last two decades or more reveals a wide variety of conflicting and contradictory testing protocols […]." ISO/IEC 19795-1:2006, S. vi.

[268] Das erste Dokument der 19795er Reihe wurde beispielsweise im Jahr 2016 einem erneuten Review unterzogen.

- vier Dokumente der Reihe »29109 – Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794« (bestehend aus derzeit zehn Dokumenten – hauptsächlich erstellt und gepflegt durch die *Working Group* 3 »Biometric data interchange formats«), soweit sie allgemeine Hinweise zu den Konformanztests und Fingerbilddaten betreffen, und
- ein Dokument der Reihe »24709 – Information technology – Conformance testing for the biometric application programming interface (BioAPI)« (bestehend aus derzeit drei Dokumenten – hauptsächlich erstellt und gepflegt durch die *Working Group* 2 »Biometric technical interfaces«), das allgemeine Hinweise zu den Schnittstellenkonformanztests enthält.

Einige wichtige Fehlertypen der vom SC37 kanonisierten Kriterien- und Fehlerkataloge werden, um Darstellungen in der Forschungsliteratur ergänzt, in den folgenden Abschnitten vorgestellt.

> „Because of variations in the way a biometric sample is captured, two templates from the same biometric will never be identical. This is the origin of the probabilistic nature of biometrics, as the matching process can only give a decision confidence, not an absolute assurance […]."[269]

Mit Verweis auf einen Text von Jain et al.[270] benennen Maltoni et al. als drei Hauptgründe für Systemfehler Beschränkungen in der Anzahl distinktiver Informationen einer biometrischen Charakteristik (*Information Limitation*), Beschränkungen in der formalen Repräsentation dieser Informationen (*Representation Limitation*) sowie in der formalen Modellierung des Spielraums, der innerhalb der verschiedenen Erscheinungsformen einer Charakteristik desselben Users liegt (*Invariance Limitation*):

> „[…] the ideal representation scheme should be designed to retain all the invariance as well as discriminatory information in the sensed measurements […;] the design of an ideal matcher should perfectly model the invariance relationship among different patterns from the same class (user), even when imaged under different presentation conditions."[271]

Sie fassen zusammen, dass die zentrale Herausforderung eines biometrischen Systems darin bestehe, mit wenigen Samples, die unter inkonsistenten Bedingungen erfasst werden, zu einer realistischen und unveränderlichen Repräsentation einer biometrischen Kennung zu gelangen und formal die charakteristische Information des Signals abzuschätzen. Besonders in Identifizierungssystemen sei dies eine schwierige Aufgabe.

[269] Dunstone und Yager 2009, S. 14.

[270] Siehe Jain, Pankanti u. a. 2004.

[271] Maltoni u. a. 2009, S. 12.

Kein Mustererkennungssystem ist fehlerfrei, da zwei Signale auch von ein und derselben Quelle nie deckungsgleich, sondern lediglich ähnlich sind und jede Umgebungs- und Systemkomponente sowie die verschiedenen Aufnahmezeitpunkte dessen Qualität beeinflussen. Daher charakterisieren statistische Performanzkenndaten die spezifische Leistungsfähigkeit eines Systems. Sie helfen dabei, biometrische Systeme untereinander zu vergleichen. Zudem werden typische statistische Performanzmetriken für das Tuning und Training der Klassifikatoren der Systeme genutzt. Die meisten Systemfehlervariablen beziehen sich auf die Module Datenerfassung, Merkmalsextraktion und Vergleich sowie die Verarbeitungsgeschwindigkeit des Gesamtsystems.

Erkennungs- und Vergleichsfehlerraten

> „In practice, a biometric system is a pattern recognition system that inevitably makes some incorrect decisions."[272]

Es mag zunächst irritierend anmuten, aber absolute Deckungsgleichheit zweier biometrischer Muster gilt als klares Zeichen für eine Manipulation etwa durch Einschleusen eines falschen Templates.[273] Eine biometrische Mustererkennung kann nur dann nicht manipuliert sein, wenn zwei Muster nicht exakt identisch sind. Dies galt bereits in der Bertillon'schen Anthropometrie, wie Cole herausarbeitet:

> „[Bertillon] viewed an exact correspondence of results as a sign of error: 'An ABSOLUTE similarity in the figures […] would be an infallible indication of a mistake.' Variations between measurements were signs of authenticity."[274]

Das heißt, die Fehler, die dadurch entstehen können, dass eine Mustererkennung eben gerade die Ähnlichkeit zweier nicht exakt deckungsgleicher Muster misst, sind auch prinzipiell ein Anzeichen dafür, dass sie auf der gerade erläuterten Ebene ungestört funktioniert. Nichtsdestotrotz stellen die Vergleichsfehler eine problematische Herausforderung dar, da sie zu Falscherkennungen führen, die im Alltag je nach Anwendungsszenario folgenschwer sein können.

---

[272] Ebd., S. 11.

[273] So weisen etwa Dunstone und Yager auf zwei Arten von *Replay*-Attacken hin, die die Signalverarbeitung des Fingerabdruckscanners oder auch des Feature-Extraction-Systems abfangen sollte. Von latenten Fingerabdrücken nachgebaute Attrappen könnten relativ leicht erkannt werden, da sie nahezu identisch mit einem schon einmal benutzten Finger seien, wenngleich dies häufig dennoch nicht geprüft würde. (vgl. Dunstone und Yager 2009, S. 255, 259). Noch einfacher dürfte die Erkennung von Replay-Attacken mit im *Transmission Subsystem* abgefangenen Samples oder Templates, die hundertprozentig identisch sind, sein.

[274] Cole 2001, S. 71 f., Hervorhebung im Original. Cole zitiert hier eine Fußnote Bertillons, in der dieser darauf hinweist, dass es auf die Höhe der zwangsläufigen Messabweichungen ankomme, die bestimmte Näherungsgrenzen nicht überschreiten dürfe (vgl. Bertillon 1896, S. 24 f.).

Ein zentrale Voraussetzung für die korrekte Messung von Vergleichsfehlern ist die *Ground Truth*. Die Testverantwortliche (*Experimenter*) eines solchen Experiments muss sicherstellen, dass bekannt ist, ob ein biometrischer Testdatensatz und eine biometrische Referenz entweder von derselben biometrischen Charakteristik derselben betroffenen Person stammen (sie *gepaarte* Teile/*mated* sind) oder ob dies nicht der Fall ist (die Teile sind dann *nicht-gepaart* bzw. *non-mated*). Kann man diese Zuordnung mittels Personenidentifikatoren für jedes Sample im Rahmen eines kontrollierten Enrolments gewährleisten, ist dies unproblematisch. In einem Real-Life-Szenario ist dies allerdings nicht realistisch.[275]

Die Vergleichsfehler lassen sich als Werte der sogenannten *Wahrheitsmatrix* (*Confusion Matrix*) angeben, mit der sich die binäre Klassifikation des Entscheidungsmoduls (*Match*/*Non-match*) quantitativ bewerten lässt.[276]

Für ein Biometriesystem sieht eine solche Wahrheitsmatrix wie folgt aus:

	biometrische Probe und biometrische Referenz stimmen überein	biometrische Probe und biometrische Referenz stimmen nicht überein
biometrische Probe und Referenz stammen von ein und derselben Person	true positive TRUE MATCH	false negative FALSE NON-MATCH *Fehler 2. Art* (*Type-2-Error*)
biometrische Probe und Referenz stammen nicht von ein und derselben Person	false positive FALSE MATCH *Fehler 1. Art* (*Type-1-Error*)	true negative TRUE NON-MATCH

Diese Fehler beziehen sich insbesondere auf die Komponenten für Vergleich und Entscheidung und werden wie folgt bestimmt:

- Die *Falschübereinstimmungsrate* (*False Match Rate*, FMR) ist der Anteil an falschen Übereinstimmungen von biometrischer Probe und biometrischer Referenz zweier verschiedener Personen an der Gesamtanzahl von Vergleichen nicht zusammengehörender biometrischer Daten im Rahmen eines Performanztests.

- Die *Falschnichtübereinstimmungsrate* (*False Non-Match Rate*, FNMR) ist der Anteil an falschen Nicht-Übereinstimmungen von biometrischer Probe und biometrischer Referenz von ein und derselben Person an der Gesamtanzahl von zusammengehörenden biometrischen Daten im Rahmen eines Performanztests.

[275] Vgl. Dunstone und Yager 2009, S. 91. Im *Abschnitt: Grenzen der Aussagekraft statistischer Fehler* (S. 101) wird auf dieses Problem noch vertiefend eingegangen.

[276] Vgl. Fawcett 2006.

Wird also von einer FMR von 0,01 Prozent gesprochen, werden bei 100.000 Vergleichen bis zu 100 falsch-positive Zuordnungen vorgenommen. Das Verhältnis von der Anzahl falsch-positiver zur Anzahl korrekter Übereinstimmungen beeinflusst entscheidend die Wahrscheinlichkeit für die reale Aussagekraft einer Übereinstimmung. Allerdings ist diese Zahl ohne Informationen über die Testdatenbasis (z. B. wie viele verschiedene Personen wurden getestet?) und das konkrete Vorgehen (z. B. ob Mehrfachversuche gezählt werden oder nicht) nicht allzu aussagekräftig. Hier kommt es erheblich auf eine gute Dokumentation der Testbedingungen an.

In der Praxis werden *False Acceptance* (*biometrische Falsch-Akzeptanz*, Häufigkeit angegeben mit FAR) und *False Rejection* (*biometrische Falsch-Rückweisung*, Häufigkeit angegeben mit FRR) oft synonym mit *False Match* bzw. *False Non-Match* oder anstatt dieser verwendet, während dies in den ISO/IEC-Normen inzwischen klar unterschieden wird.[277] FMR/FNMR beziehen sich lediglich auf die Entscheidung des Entscheidungsmoduls in Bezug auf die reale Übereinstimmung, die natürlich bekannt sein muss (*Ground Truth*). FAR/FRR beziehen sich auf den Anwendungskontext. So kann eine falsche Übereinstimmung im Falle eines Systems, das doppelte Identitäten verhindern soll, zu einer Falschrückweisung führen, während es in einem Zugangskontrollsystem zu einer falschen Akzeptanz führt.[278] Sobald Falschakzeptanz- und Falschrückweisungsrate angegeben werden, muss zusätzlich berücksichtigt werden, dass sie durch ihre Kontextgebundenheit abhängige Wahrscheinlichkeiten wiedergeben. Das heißt, die Wahrscheinlichkeit, dass jemand, der vom System erkannt wurde, auch tatsächlich die erkannte Person ist, ist abhängig davon, wie hoch die Wahrscheinlichkeit dafür ist, dass Menschen das System hintergehen – eine schwer unter Laborbedingungen zu erfassende Größe.

Gegenseitige Abhängigkeit der Vergleichsfehlerraten

Es ist von großer Bedeutung, dass FMR/FNMR bzw. FAR/FRR einander bedingen. In Abbildung 3.3 ist dies für eine fiktive Wahrscheinlichkeitsverteilung des Ähnlichkeitswerts s (*Similarity Score*) im Intervall [0,1] einer Anzahl n fiktiver Testvergleiche veranschaulicht. In diesem Beispiel werden bei der Hälfte der Testvergleiche zwei Templates von demselben Finger (sogenannte *Genuine Attempts*) und bei der anderen Hälfte zwei Templates von verschiedenen Fingern (sogenannte *Impostor Attempts*) in einem Verifikationssystem verglichen. Die zwei Kurven geben hier die Verteilungen der Wahrscheinlichkeiten für die jeweilig gemessenen Vergleichswerte an. In der Regel ist der Ähnlichkeitswert nahe 1 bei hoher Übereinstimmung, bei 0 bei niedriger Übereinstimmung – dementsprechend liegt die Kurve mit der Verteilung der Vergleiche der Bilder

[277] Siehe ISO/IEC 19795-1:2006, S. 13. Im ISO/IEC 2382-37:2017 werden *False Acceptance* und *False Rejection* als Teile des interaktions- und nicht des performanzbezogenen Vokabulars geführt.

[278] Vgl. Maltoni u. a. 2009, S. 15.

nicht-identischer Finger weiter links als die mit denen der Bilder identischer Finger. Die beiden Kurven überlagern sich etwas zwischen den Vergleichswerten 0,4 und 0,6. Hier kann es passieren, dass eine Falscherkennung entsteht. Je nachdem auf welchen Ähnlichkeitswert nun die Schwelle t (*Threshold*) gesetzt wird, anhand derer über *Match* ((s<t)) oder *Non-Match* ((s>t)) entschieden wird, erhöht sich entweder die Wahrscheinlichkeit für falsch-negative oder für falsch-positive Erkennungen.

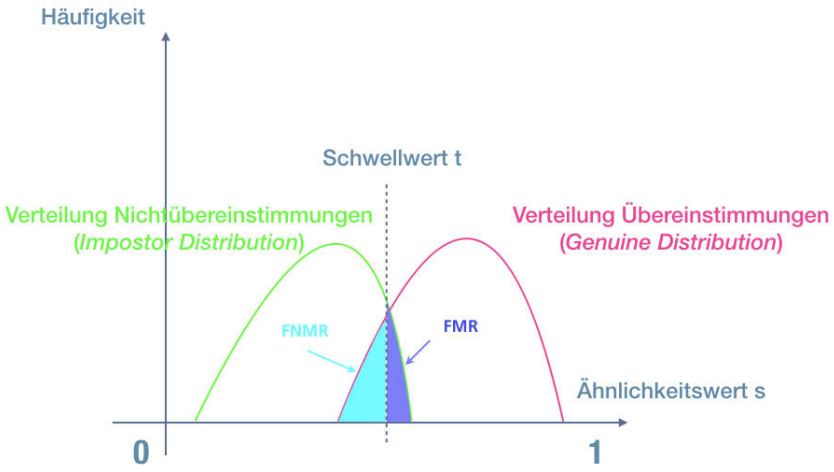


Abbildung 3.3: Fiktive Wahrscheinlichkeitsverteilung der Ähnlichkeitswerte von Vergleichen von Referenz und Probe identischer Finger (rechte Kurve) und nicht-identischer Finger (linke Kurve); Abbildung angelehnt an Maltoni u. a. 2009, S. 17.

Man spricht in diesem Zusammenhang von einem *Tradeoff* zwischen beiden Fehlerraten. Die Entscheidungsschwelle ließe sich auf die Abbildung bezogen beispielsweise so weit nach rechts setzen, dass die Wahrscheinlichkeit für einen *False Match* Null ist, in einem Zugangskontrollsystem beispielsweise also theoretisch niemand fälschlicherweise durchkommt – mit dem Nachteil, dass die höchstmögliche Anzahl an fälschlichen Rückweisungen auftritt. Ein Zugangssystem ist dann aus administrativer Sicht sehr sicher eingestellt, führt aber zu erheblicher Nutzerinnenfrustration. Im entgegengesetzten Fall – die Schwelle wird so weit nach links gesetzt, dass die Wahrscheinlichkeit, dass eine falsche Zurückweisung auftritt, bei Null liegt – wird die höchstmögliche Falschpositivrate in Kauf genommen. Das System gilt nun als sehr tolerant.

Kurz gesagt: Wenn die FMR sinkt, dann steigt die FNMR und umgekehrt.

Es gibt stets auch den Punkt, an dem beide Fehlerraten gleich groß sind, die sogenannte *Equal Error Rate* (EER). Die Wahl des Schwellwerts orientiert sich allerdings weniger daran, sondern am Anwendungskontext der Applikation:

> „For example, a biometric portal can be effective with even a 20 % false match rate (an 80 % probability of intercepting an impostor), which may be low enough to decrease the frequency of attacks on the biometric system to the point that there are no successful

impostor transactions. Truly determined fraudsters might find other entry points, including the exception handling mechanism, more appealing than the biometric portal. Conversely, in a criminal identification system a false match may result in a false arrest or imprisonment, so false match rates must be reduced as much as possible."[279]

Grenzen der Aussagekraft statistischer Fehler

Eines der bereits erwähnten Grundprobleme einer erfolgreichen Performanzevaluation ist die Schwierigkeit, *vor* dem System zu wissen, welche biometrischen Muster zusammengehören und welche nicht. Diese Grundwahrheit (*Ground Truth*) ist nötig, um überhaupt bewerten zu können, dass das System richtig oder falsch entschieden hat – ein unbemerkter Fehler ist statistisch irrelevant.

„While the [similarity] score determines whether the user is accepted by the laptop, it does not indicate if it is actually a genuine or impostor match. In fact, an operational algorithm never knows for certain if it is seeing an impostor (as they don't usually identify themselves), so the system must rely only on the score to make its decision."[280]

Das initiale Bezeugen der Identität einer Person ist also wichtig, um die in der statistischen Modellierung wichtige *Ground Truth* abzusichern:

„To test the fingerprint algorithm both impostor and genuine matches must be conducted to work out the chance of an incorrect result. During testing it is known whether matches are impostor or genuine, so the scores can be appropriately labeled. The labeling of matches as impostor or genuine is known as establishing *ground truth*."[281]

In einer operationalen Evaluation ist dies so nicht möglich, da hier nur die Identitätsbehauptung bekannt ist, die sich nicht zwangsläufig mit der „wahren Identität" deckt.[282] Eine manuelle Identitätsprüfung durch das Heranziehen anderer Identitätsdokumente oder Zeugen ist hier eine Abhilfe, die das Problem in einem gewissen Maße nur verschiebt, erheblichen Mehraufwand bedeutet und unangenehm für die Nutzerinnen ist. Um jedoch eine korrekte Wahrscheinlichkeit dafür anzugeben, wie *wirksam* ein System in einem konkreten Szenario etwa hinsichtlich der Aufdeckung falscher Identitätsbehauptungen ist, ist es unablässlich, mindestens eine gut begründete Schätzung über deren reales Auftreten im konkreten Anwendungskontext – die Prävalenz – abzuge-

[279] ISO/IEC TR 24741:2007, S. 14. Ein weiteres mögliches Szenario ist das von der Datenschützerin Marit Hansen auf einer Tagung der Humboldt-Universität geschilderte. Hier senkte eine Bank für einen kurzen Zeitraum den Schwellwert des testweise eingesetzten Biometrie-Systems eines Geldautotmaten so weit herab, dass sie *False Matches* zugunsten einer FNMR von Null in Kauf nahm, um keine Kunden mehr wegen zu vieler Falschrückweisungen zu verprellen (vgl. Knaut 2013, S. 74 f.).

[280] Dunstone und Yager 2009, S. 31.

[281] Ebd.

[282] Dunstone, Yager verwenden hier den Begriff „true identity", Ebd., S. 91.

ben. Sobald die Prävalenz des erwarteten Ereignisses unter der Falschpositivrate liegt, kann der Einsatz zu erheblich vielen falschen Anschuldigungen führen.

Dieses mit der Bedingtheit von FMR/FNMR zusammenhängende Problem, das sich aus dem Bayes-Theorem ergibt, wird selten ausführlich im Rahmen von allgemeinen Darstellungen zu den Systemfehlern der Biometrie erklärt. Eine Ausnahme bildet hier die Einführung in biometrische Konzepte der von DARPA, DHS und CIA finanzierten Studie »Biometric Recognition« des *Whither Biometrics Committee*, in der es zum Missverstehen der Fehlerraten heißt:

> „It seems intuitively obvious that a declared nonmatch in a biometric system with both FMRs and FNMRs of 0.1 percent is almost certainly correct. Unfortunately, intuition is grossly misleading in this instance, …“[283]

Studien in anderen Disziplinen haben gezeigt, dass bedingte Wahrscheinlichkeit auch unter Expertinnen häufig nicht einfach so verstanden wird.[284] Eine mögliche Veranschaulichung mit Hilfe von Entscheidungsbäumen kann hier helfen. Diese und die zusätzliche Verwendung ganzer Zahlen statt Prozentangaben lassen einfacher nachvollziehen, dass die biometrischen Fehlerraten nur bedingt etwas darüber aussagen, inwiefern ein Treffer in einem bestimmten Anwendungskontext *wirklich* einer ist.

Im Beispiel in Abbildung 3.4 betrage die Prävalenz, dass in einer gegebenen Menschenmenge jemand terrorverdächtig ist, 0,0001 % – das heißt, dass einer von einer Million terrorverdächtig ist. Haben wir nun ein Fingerabdruckerkennungssystem mit einer Erkennungsgenauigkeit von 99,5 % und einer FMR von 0,1 %, dann wird die eine terrorverdächtige Person zwar relativ sicher, aber 1000 von 999.999 Menschen werden fälschlicherweise als terrorverdächtig erkannt. Die Wahrscheinlichkeit dafür, dass jemand, die als terrorverdächtig erkannt wurde, auch real eine Terroristin ist, liegt also bei rund 0.1 % – der Einsatz eines solchen Systems würde zu schwerwiegenden Verdächtigungen bei geringer Wirksamkeit führen.[285]

Anders gelagert ist der Fall, wenn wir ein mit Eurodac vergleichbares System haben (Abbildung 3.5). Das ebenfalls mit fiktiven Zahlen arbeitende Szenario sei wie folgt gegeben: Von 100.000 Menschen dürfen 10 % nach geltenden Regeln keinen Asylantrag stellen, weil sie schon einmal einen woanders gestellt haben. Angenommen, die FMR des Systems liegt auch bei 0,1 % und die Erkennungsgenauigkeit bei 99,5 %.[286] Von

[283] Pato und Millett 2010, S. 37. In einem Vortrag auf der *Biometrics Consortium Conference* sprach Wayman, eines der 13 Mitglieder des Komitees, vom „Problem of Rev. Bayes“ (vgl. Wayman 2013, S. 25).

[284] Insbesondere in Medizin und Psychologie ist das Problem seit geraumer Zeit ein Thema. Siehe hierzu bspw. Gigerenzer und Hoffrage 1995.

[285] Die Abbildungen sind analog zu den Beispielen in einem Vortrag vom *Director Government Solutions* von *L-1 Identity Solutions* Norbert Wendt in Bezug auf Gesichtserkennungsszenarien erstellt, dem ich für die Bereitstellung seiner leider unveröffentlichten Folien danke. Wendt o. J.

[286] Nach den in *Kapitel 1.1* für Eurodac genannten Anforderungen hat das System eine „accuracy $> 99.9\,\%$“. Diese drückt das Verhältnis der Summe korrekter *Matches* und *Non-Matches* zur Gesamt-

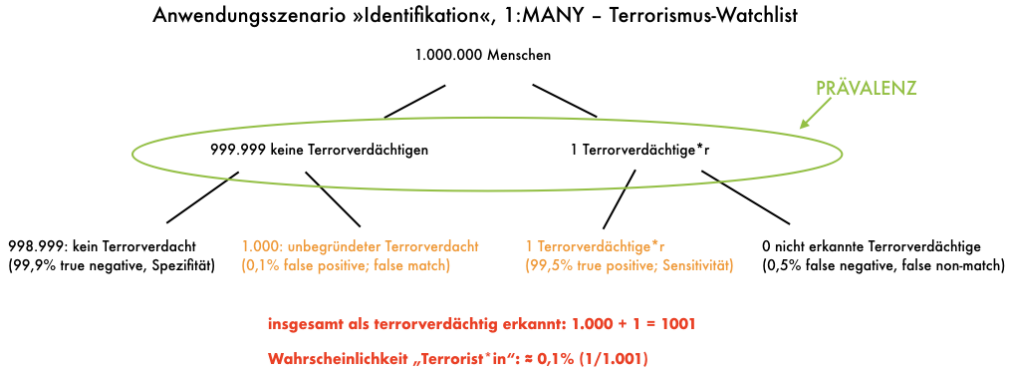


Abbildung 3.4: Entscheidungsbaum – fiktives Szenario „Terrorismus-Watchlist“; angelehnt an Wendt o. J., S. 15 f.

den 90.000, die Asyl beantragen dürfen, werden 90 fälschlicherweise als nicht dazu berechtigt sowie 9.950 den Regeln gemäß korrekt als unberechtigt erkannt. Die Wahrscheinlichkeit, dass jemand, die als unberechtigt erkannt wird, auch den Regeln nach tatsächlich unberechtigt ist, liegt hier also bei 99,1 % – das System arbeitet effektiv aus Sicht der gestellten Aufgabe, aber keinesfalls fair.[287] Jenseits dessen überlagert die Berechnung die wichtigere Frage nach der Legitimität dieser Selektion an sich.

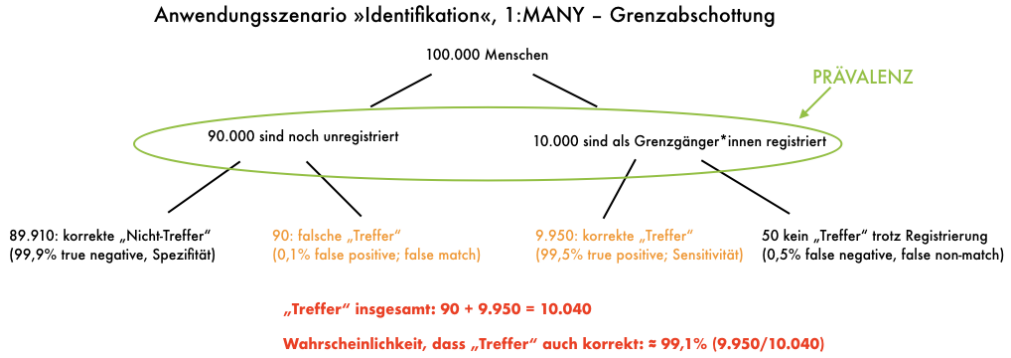


Abbildung 3.5: Entscheidungsbaum – fiktives Szenario „Grenzabschottung“; angelehnt an Wendt o. J., S. 12 f.

zahl der vermessenen Personen aus. Die Anzahl der korrekten *Matches* wiederum ist abgeleitet aus der Anforderung einer „probability of $< 0.5\,\%$ of missing a match“ (FNMR). Es ließen sich keine wissenschaftlichen Belege dafür finden, dass Eurodac diese Werte real erreicht.

[287] Den falsch positiv Erkannten droht Abschiebung. Töpfer erwähnt, dass auch falsch negativ Erkannte von Problemen betroffen sind. Dies illustriere der Fall zweier somalischer Schwestern, die 2012/13 „zusammen über Italien und Österreich nach Deutschland eingereist waren, dann aber auf unabsehbare Zeit getrennt wurden, als nur eine Schwester aufgrund eines Eurodac-‚Treffers‘ nach Italien zurückgeschoben wurde, die andere mangels ‚Treffers‘ jedoch nach Österreich.“ (Töpfer 2015, S. 66).

Fehlerraten bei der Datenerfassung

> „The sensor module defines the human machine interface and is, therefore, pivotal to the performance of the biometric system. A poorly designed interface can result in a high failure-to-acquire rate [...] and, consequently, low user acceptability."[288]

Als *Failure to Capture* (FTC) bezeichnet man das Misslingen des „*biometrischen Erfassungsprozesses* ein *biometrisches Sample* zu erstellen".[289] Das kann beispielsweise heißen, dass das erstellte Bild leer, weiß oder von sehr schlechter Qualität ist. Bei einem FTC kommt es zu einem Erfassungsprozess, der aber fehlschlägt. Dem vorausgehend kann es bereits sein, dass der Sensor gar nicht auf einen an ihm befindlichen Finger reagiert. Dies wird als *Failure to Detect* (FTD) bezeichnet. Die Rate von FTD ist gewöhnlich umgekehrt proportional zur Rate der FTC.[290]

Faktoren, die die Fingerabdruckqualität beeinflussen, können die Hautbeschaffenheit, Sensorqualität und -bedingungen, Nutzerkooperation oder die korrekte Benutzung des Sensorgeräts sein.[291]

Qualitätsanforderungen an die Bilddaten und ihre Messung Die Qualität der Sensortechnik und der mit ihnen erzeugten Bilder ist von entscheidender Bedeutung für einen korrekt ablaufenden biometrischen Vergleichsprozess im jeweiligen Anwendungskontext. Ein einfaches Beispiel ist die Größe der gescannten Bildfläche. So sind die Fingerbilder sämtlicher kommerzieller Scanner zu klein für kriminalistische Anwendungen. In den nuller Jahren beispielsweise wurden bevorzugt die kostengünstigeren und kleineren Solid-State-Sensoren in Massenware verbaut, aber sie produzieren aus kriminaltechnischer Perspektive ungenügende Bilder.[292]

Lumini et al. benennen die *Fingerprint Quality* als „a measure of the clarity of ridge and valley pattern, but it is not simple to describe it with mathematical equations".[293] Entsprechend führen sie auch keine mathematischen Gleichungen an, sondern verweisen auf Maschinenlerntechniken für das Training der Parameter von Funktionieren, die die Einschätzung einer guten Fingerabdruckqualität abbilden.

Mittels diverser Standards der Industrie, nationaler wie internationaler Normungsinstitutionen sowie technischer Richtlinien der Polizeien wurden konkrete Prüfkrite-

[288] Jain, Flynn und Ross 2008a, S. 3, 10.

[289] Dt. Übersetzung von: „failure of the *biometric capture process* to produce a *captured biometric sample*" (ISO/IEC 2382-37:2017, S. 20, Hervorhebung im Original), zu finden bei Busch o. J. (siehe auch Bemerkung Fußnote 74).

[290] Vgl. Maltoni u. a. 2009, S. 13.

[291] Vgl. Lumini, Nanni und Maltoni 2010, S. 341.

[292] „No commercially available single-finger solid state scanner meets these image size [of NIST: $16.5mm^2$/at least 320x320px] requirements." (Wasserman 2005, Folie 7).

[293] Lumini, Nanni und Maltoni 2010, S. 341.

rien etabliert, die bei einer Systemimplementierung abgearbeitet werden können. Die wichtigsten Dokumente innerhalb Deutschlands und der EU sowie der USA werden im Folgenden aufgezählt und kurz erläutert:

- Ein zentraler Referenzpunkt der im Folgenden erwähnten Standards ist der Appendix F »FBI/CJIS Image Quality Specifications« der »Electronic Biometric Transmission Specification« (EBTS) der *Criminal Justice Information Services Division* (CJIS) des FBI. Häufig findet sich noch der Verweis auf die rein auf Fingerbiometrie bezogene »Electronic Fingerprint Transmission Specification« (EFTS), deren letzte Version 7.1 im Jahr 2005 erschien. Mit Version 8 erweiterte man die Spezifikation ab Mitte 2007 mit Blick auf die sich rasant entwickelnde „biometric identification industry“ um Austauschformate für Bilder anderer biometrischer Modalitäten wie zum Beispiel Iris, Gesicht oder Handabdruck.[294] Inzwischen gibt es seit Mitte 2013 die zehnte Version,[295] die sich in großen Teilen mit der alten gleicht, aber um Anforderungen für mobile Fingerprint-Scanner erweitert wurde.

- Die Empfehlungen des FBI stehen im Einklang mit denen des NIST sowie des ANSI-akkreditierten INCITS. Hierzu gehört der ANSI/NIST-ITL 1.

- Auf internationaler Ebene hat das SC37 zum Beispiel Folgendes publiziert:
  - »Information technology — Biometric sample quality — Part 4: Finger image data« (ISO/IEC TR 29794-4),
  - »Information technology — Biometric data interchange formats — Part 4: Finger image data« (ISO/IEC 19794-4:2011) mit Ausführungen zu „Image Acquisition Requirements“ und mehreren Anhängen zu Qualitätsanforderungen an das Aufnahmegerät, die Bildqualitätsprüfungssoftware und die Bildkompression.

- In Deutschland hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) »Qualitätsanforderungen bei der Erfassung und Übertragung der Fingerabdrücke als biometrische Merkmale für elektronische Pässe« als Teil der »Technischen Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für hoheitliche Dokumente« spezifiziert.[296]

- Die Standards des Normenausschusses »Informationstechnik und Anwendungen« (NIA) im Deutschen Institut für Normung (DIN) sind stark an die der ISO/IEC angelehnt.

[294] Siehe CJIS 2007, S. 2.

[295] Siehe CJIS 2013. Seitdem sind mehrere kleinere Revisionen dieser Version erschienen.

[296] Annex 2, auch »QS-Finger« genannt, der TR-03104, auch TR-PDÜ genannt.

Probleme der Sensortechnik Ein grundsätzliches Problem der sensorischen Erfassung der Hautoberfläche ist das schlechte mechanische Signal-Rausch-Verhältnis, das von den vielen möglichen Zuständen der Haut beeinträchtigt wird oder auch sensorspezifisch sein kann.[297] Zum Beispiel haben sich die frühen kapazitiven Sensoren der 1990er Jahre als unzuverlässig und schlecht benutzbar erwiesen,[298] sobald sie mit Haut in Berührung kamen, die trocken, schwitzig, verletzt oder verschmutzt war oder die Schwielen hatte. Auch die Haut älterer oder gestresster Menschen sowie die Einnahme bestimmter Medikamente hatten erheblichen Einfluss auf die Zuverlässigkeit dieser Sensoren.

Viele Probleme gibt es auch mit den Sweep-Sensoren, die wegen ihrer kostengünstigeren, da kleineren Sensorfläche oder ihrer besseren Eignung zum Beispiel bei thermischen Techniken stark verbreitet sind. Die Anforderungen an User-Training, Bildverarbeitung oder zusätzliche Sensorik, um die nicht vorherzusehende Geschwindigkeit des Fingers, der über den Sensor gleitet, sinnvoll aufzufangen, sind entsprechend etwas höher als bei Touch-Sensoren. Andererseits sind sie lange Zeit kleiner und billiger gewesen, und es gibt keine latenten Rückstände auf dem Sensor.

Fehlerraten bei der Merkmalsextraktion

Der Übergang zwischen Fehlern der Datenerfassung und Merkmalsextraktion ist fließend, je nachdem, ob man Bildvorverarbeitung, -qualitätsprüfung und -verbesserung noch dem Erfassungsmodul oder bereits komplett der *Feature Extraction* zuordnet.[299]

So schreiben Maltoni, Maio, Jain und Prabhakar, dass der sogenannte *Failure to Acquire* (FTA), den sie als Fehler des Feature-Extraction-Moduls klassifizieren, eine Kombination aus FTC, FTD und *Failure to Process* (FTP) sei.[300] Mit der FTA-Rate wird der Anteil gescheiterter Erfassungsversuche eines Merkmals an einer spezifizierten Gesamtmenge von Erfassungsversuchen bezeichnet. Das Scheitern allerdings bezieht sich darauf, dass die Qualität der erfassten Daten nicht den administrativen Systemregeln für eine Weiterverarbeitung entspricht.[301] Das heißt, ein FTA kann nur auftreten, wenn ein Sample produziert wurde, also keine Erfassungsfehlfunktion aufgetreten ist. Eine hohe FTA-Rate beeinflusst die *Throughput Rate* des Gesamtsystems und führt zu Unzufriedenheit bei den Nutzerinnen.[302] Eine höhere Sensitivität der Capture- und Feature-Extraction-Module, um die FTA zu senken, erschwert die Arbeit der später

[297] Vgl. Setlak 2004, S. 34.

[298] Vgl. ebd.

[299] Siehe hierzu auch *Kapitel 4.2 Unterschiede in der Beschreibung der Systemarchitektur* (S. 144).

[300] Vgl. Maltoni u. a. 2009, S. 14. Der bisher noch nicht erwähnte FTP tritt auf, wenn es nicht möglich ist, aus dem eingangs erfassten Bild eine benutzbare Merkmalsmenge zu extrahieren.

[301] Vgl. ISO/IEC 2382-37:2017, S. 19.

[302] Vgl. Maltoni u. a. 2009, S. 14.

folgenden Module/Prozesse wie bspw. des Matching-Moduls.[303] Jain, Flynn und Ross ordnen den FTA der Datenerfassung zu und verwenden ihn synonym zum FTC.

Maltoni et al. fassen zudem den Prozess des Template-Enrolments, in dem Datenerfassung, Merkmalsextraktion und Speicherung vorkommen, als *Template Creation Module* auf, bei dessen funktionalem Scheitern der *Failure to Enrol* (FTE) auftritt.[304]

Manchmal werden Fehler wie die FTE-Rate auch ignoriert. Eine mögliche Abschaltung des FTE bedeute beispielsweise einfach nur, dass „noisy templates" entstehen würden, die zu höheren Matching-Fehlern führten. Es gibt einen Kompromiss zwischen FTE und den Fehlerraten des Matching-Moduls.[305]

Im Rahmen der ISO/IEC-Standardisierung sind sowohl FTE als auch FTA als Fehlerereignisse des *BioAPI-Framework* vorgesehen. Wenn nach einer negativen Qualitätsprüfung von extrahierten Template-Daten eine gegebenenfalls erfolgende Neuerfassung eines Samples wieder zu unzureichender Qualität führt, wird einer der beiden Fehler über das Framework an die kontrollierende Applikation gemeldet. Eine Ursache für einen solchen Fehler kann zum Beispiel die fehlgeschlagene Segmentierung des Bildes sein.

Die Ursachen für eine fehlschlagende oder falsche Merkmalsextraktion können nicht selten schon in der schlechten Qualität des Samples liegen. Im Zusammenspiel mit Datenerfassungs- und Extraktionsalgorithmen, die Flecken, Narben, latente Abdrücke anderer Finger auf der Sensoroberfläche, Artefakte durch zu schwitzige oder zu trockene Haut nicht erkennen oder reparieren können, entstehen dann beispielsweise auch fehlerhafte Minutien.

Datendurchsatzraten

Eine etwas andere Größe im Rahmen der Performanzmetrik ist die *Throughput Rate*, da sie in Bezug auf Fehler einen anderen Charakter hat als die bisher genannten Variablen. Sie bezieht sich auf das gesamte System. Ein langsames System kann zum Beispiel bis hin zum Beinahe-Stillstand eine erhebliche Beeinträchtigung der Gesamtfunktionalität darstellen.

Die Antwortzeiten des Systems oder die Datendurchsatzraten hängen ganz erheblich von den Speicher-, Kompressions- und Verschlüsselungsverfahren, den Bandbreiten der Datenleitungen, dem Datenbankmanagement-System, der Rechengeschwindigkeit sowie den Template-Größen und ihrer Kodierung, aber auch von der Dauer der Mensch-Maschine-Interaktion bei der Sample-Erfassung ab. Für eine allgemeine Erfassung einer Durchsatzrate im Sinne der pro Zeiteinheit komplett abschließend verarbeitbaren Nutzeranfragen empfiehlt das SC37 beispielsweise, zum einen die Interak-

[303] Vgl. ebd.

[304] Vgl. ebd., S. 13.

[305] Vgl. ebd., S. 14.

tionszeiten der betroffenen Personen mit dem System, zum anderen – insbesondere bei Identifikationssystemen – auch die konkrete Rechenzeit des Computers mittels geeigneter Benchmark-Tests zu messen.[306]

3.2.3 Schnittstellen- und Bilddaten-Konformanzfehler

Eine andere Klasse von Fehlern sind Konformanzfehler. Dabei handelt es sich um Inkompatibilität einer konkreten Produktimplementation mit einer speziellen auf nationaler oder internationaler Ebene hierfür festgelegten Norm. Aus solchen Fehlern folgen Probleme in der Interoperabilität oder der Integrierbarkeit von Komponenten eines Systems oder aber verschiedener Systeme.

Die bereits in Ausschnitten dargestellten Normen für Datenaustauschformate und die Schnittstellen spezifischer Systemkomponenten bieten fest definierte Kriterien, die formale Konformitätsprüfungen bestimmter qualitativer Standards für Bildformate und Interoperabilität erlauben.

Beispielsweise werden seitens des SC37 international verschiedene Gruppen von Standards für technische Schnittstellen und interoperable Datenformate festgelegt:[307]

- fest definierte Meta-Datenformate im *Common Biometric Exchange Formats Framework*, die zu jedem Fingerbild oder auch den Bildern anderer biometrischer Modalitäten – kodiert im *Biometric Data Block* – als Wrapper hinzukommen,[308]
- die *Biometric Data Interchange Formats* für den je nach Modalität auf bestimmte Weise definierten *Biometric Data Record* (BDR) (im CBEFF ist das der BDB),[309]
- das *Biometric Application Programming Interface* für den Datenaustausch zwischen den von verschiedenen Herstellern stammenden Modulen eines einzigen Systems[310] sowie

[306] Vgl. ISO/IEC 19795-1:2006, S. 13.

[307] Larmouth 2009, S. 145.

[308] Die Dokumentreihe 19785 der ISO/IEC spezifiziert sämtliche Datenelemente des CBEFF, die Verfahren, um proprietäre Formatspezifikationen bei der *Biometric Registration Authority* offiziell registrieren und im CBEFF dann unter Stammformaten und ggf. mit Security-Formaten eintragen zu können. Vgl. ISO/IEC 19785-1:2015, ISO/IEC 19785-2:2006, ISO/IEC 19785-3:2015, ISO/IEC 19785-4:2010.

[309] Die Dokumentreihe 19794 der ISO/IEC spezifiziert etwa 15 verschiedene Austauschformate, darunter auch für DNA-, Venen-, Gesichts- oder Irisdaten. Für fingerbezogene Daten sind dies ISO/IEC 19794-1:2011/Amd 1:2013, ISO/IEC 19794-2:2011/Amd 1:2013, ISO/IEC 19794-4:2011/Amd 1:2013 und ISO/IEC 19794-8:2006.

[310] Die Dokumentreihe 24709 der ISO/IEC bietet drei Standards für das Vorgehen bei diesbezüglichen Konformanztests.

- das *Biometric Application Programming Interface Interworking Protocol* für den Daten- und Kontrollfluss in einem Netzwerk zwischen verschiedenen biometrischen Systemen.

Für alle standardisierten Schnittstellen- und Datenformate gibt es jeweils methodologische Empfehlungen, wie sich die Konformanz mit selbigen überprüfen lässt und Teilautomatisierungen derartiger Tests. Dies wird im Rahmen dieser Arbeit jedoch nicht weiter vertieft.

3.3 Fehler durch dynamische Körper- und Umgebungsfaktoren

> „From the signal analysis viewpoint, the image on the surface of the skin has a poor mechanical signal-to-noise ratio."[311]

Die im letzten Kapitel erläuterten Fehler in Erkennungsgenauigkeit und -geschwindigkeit können hochgradig vom Anwendungskontext, von der Messumgebung und von den körperlichen und verhaltensbezogenen Eigenschaften der Personen, die das System benutzen müssen, abhängig sein. Diese Faktoren können Fehlerursachen für ein erhöhtes Auftreten bestimmter Systemfehler sein. In den statistischen Experimental-Settings versucht man sie so zu gruppieren, dass man sie a) als unabhängige, beobachtete Variablen einbezieht, b) als durch das ganze Experiment unverändert belassene Faktoren kontrolliert, c) gezielt randomisiert oder d) explizit als zu vernachlässigende ignoriert, um die Komplexität des Experiments zu verringern.[312]
Das ideale System soll immer gleich gut in Bezug auf Änderungen von Körper, Umgebung oder Verhalten funktionieren. Es soll einzig und allein den Zweck erfüllen, immer ein und dieselbe Person wiederzuerkennen, egal wie stark diese gealtert, ob sie krank oder verletzt, ob es dunkel oder hell, kalt oder warm ist.[313] Diese „defizitären" Bedingungen sollte die Technik so gut wie möglich abfangen. Aus dieser Perspektive ist die Technik fehlerhaft, wenn sie hier nicht invariant agiert – sie macht Anpassungsfehler. Eine sehr umfassende Übersicht, die zwar keinen Anspruch auf Vollständigkeit erhebt, über bekannte Bedingungen, die umgebungs-, verhaltens-, körper- oder einsatzbedingt problematisch für geringe Systemfehlerraten sind, gibt das SC37.[314] Tabelle 3.3 zeigt die dort aufgezählten Faktoren zusammengefasst.

---

[311] Setlak 2004, S. 34.

[312] Vgl. ISO/IEC 19795-1:2006, S. 15 f.

[313] Die grundlegende Auffassung über die Identität der Person, die dem zugrundeliegt, wird als möglicher erkenntnistheoretischer Fehler unter das *Kapitel 3.5 Begriffs- und erkenntnistheoretische Probleme* (S. 119) gefasst.

[314] Im Annex C, »Factors influencing performance« in ISO/IEC 19795-1:2006, S. 46 ff.

Kategorisierung in ISO/IEC-Dok. 19795	genannte Faktoren
Demographische Daten	Alter, „ethnic origin“ [sic], Gender, Beruf
Anwendung	Template-Alterung, Tageszeit, Versiertheit im Umgang mit dem System, Nutzermotivation
Physiologie der User	Amputation, Arthritis, Blindheit, Prellungen, Quetschungen, div. Erkrankungen, Fingernagelwachstum, Tiefe und Abstand der Papillarlinien, trockene, rissige oder feuchte Finger
Verhalten der User	Versatz oder Rotation bei der Fingerpositionierung, vorherige Aktivität (schwitzige Hände), Stress, Stimmung
Aussehen der User	Bandagen/Verbände, künstliche Fingernägel
Umwelteinflüsse	Beleuchtung (insbes. bei optischen Sensoren), Temperatur, Feuchtigkeit
Sensor und Hardware	Schmutz oder latente Abdrücke auf dem Sensor, Sensorqualität, -abnutzung, Unterschiede in den Produktmodellen bei Austausch, Übertragungskanal (Routing, Networks)
User-Schnittstelle	Feedback an den Nutzer (gescannter Fingerabdruck in seiner Qualität sichtbar?), Nutzerführung und -training

Tabelle 3.3: Liste von Faktoren, die im realen Betrieb von Biometriesystemen die Performanz beeinflusst haben. Zusammenfassung der Angaben in ISO/IEC 19795-1:2006, S. 46 ff., von Verfasserin übersetzt.

Viele der genannten Punkte werden zudem häufig auf der Ebene bestimmter Verhaltensregeln im Umgang mit dem System beeinflusst. Auch das Kooperationsverhalten der betroffenen Personen beeinflusst die Effektivität des Systems maßgeblich:

> „In systems where a subject seeks verification of a positive claim to an enrolled identity, the subject can cooperatively present the characteristic to the sensor. The act of presenting a biometric characteristic to a sensor introduces a behavioural component to every biometric method as the subject must interact with the sensor in the collection environment.“[315]

Gerade wenn biometrische Systeme in unfreiwilligen Szenarien („overt, non-cooperative application“)[316] eingesetzt werden, wird mit Nutzungsregeln und entsprechendem Betreuungspersonal zusätzlich sichergestellt, dass ein gleichbleibendes Kooperationsverhalten der User vorliegt.

Im Jahr 2008 hat das SC37 den vor allem von der *Working Group* 6 »Cross-Jurisdictional and Societal Aspects of Biometrics« erstellten *Technical Report* »Biometrics – Jurisdictional and Societal Considerations for Commercial Applications – Part 1: General Guidance« veröffentlicht. Das Dokument richtet sich an „planners, imple-

[315] ISO/IEC TR 24741:2007, S. 10.

[316] „If a system is to be used in an overt, non-cooperative application, the user must not be able to willfully change the biometric or its presentation sufficiently to avoid being matched to previous records.“ (Wayman, Jain u. a. 2005, S. 10).

menters and system operators of biometric systems“[317] und enthält Empfehlungen und Richtlinien, die den gesamten Lebenszyklus eines biometrischen Systems betreffen sollen und damit bereits im Design vorgedacht werden müssen. Die Vorgaben behandeln rechtliche und gesellschaftliche Beschränkungen für die Nutzung biometrischer Daten, Maßgaben zur Zugänglichkeit für den größtmöglichen Teil der Bevölkerung sowie Gesundheits- und Safety-Probleme, die auf die Besorgnisse der Nutzerinnen hinsichtlich potentieller Gefahren sowie Möglichkeiten des Missbrauchs von biometrischen Informationen abgeleiteter Daten abheben.[318] Es werden hiermit teilweise Kritiken aus sozial-, politik- oder rechtswissenschaftlichen und ethischen Studien aufgegriffen und in Designanforderungen übertragen. Allerdings gehen viele Analysen anderer Disziplinen weit darüber hinaus, als dass sie einfach nur in Verbesserungsanforderungen des Systemdesigns übertragen werden können. Das eben genannte und weitere ISO/IEC-Dokumente[319] ähnlicher Art sind, laut Darstellung in eben diesen Dokumenten, dafür gedacht, die Akzeptanz biometrischer Systeme und die öffentliche Wahrnehmung, das Verständnis für ein gutes Design dieser Systeme, das Bewusstsein bezüglich Problemen mit Barrierefreiheit und die Übernahme allgemein anerkannter guter Datenschutzpraxis zu befördern. Sie sollen zudem die Einführung und den Betrieb der Systeme problemloser gestalten und die Langzeitkosten reduzieren.[320]

3.4 Überwindungsfehler

Die dritte Fehlergruppe, die zumindest in jüngerer Zeit zu der am häufigsten in der Biometrie beforschten gehört, sind die *Security Failures*. In diesem Bereich werden vor allem unerwünschte Interaktionen zwischen umfangreich typisierten Nutzerinnen und dem System beschrieben.

Ein biometrisches Fingerabdruckerkennungssystem kann wie jedes Computersystem entweder willentlich initiiert oder durch ungeeignete, nicht antizipierte Nutzungsweisen, Umwelteinflüsse sowie nicht abgefangene, kritische Softwarefehler komplett ausfallen, unerwartet oder unerwünscht reagieren. Fehlfunktionen oder Ausfall durch Manipulationen werden als Bedrohungen (*Threats*) aufgefasst. Als typische Bedrohungen gelten *Denial-of-Service* (Systemüberlastung und damit verbundener Ausfall), *Circumvention*/*Intrusion* (ein vorsätzliches Eindringen in das System durch eine nicht dazu autorisierte Nutzerin), *Function Creep* (eine Erfassung und Nutzung biometrischer

[317] ISO/IEC TR 24714-1:2008, S. 1.

[318] Vgl. ISO/IEC TR 24714-1:2008, S. 1.

[319] Hierzu gehören ISO/IEC 24779-1:2016, ISO/IEC 24779-4:2017, ISO/IEC TR 30110:2015 und das in Entwicklung befindliche ISO/IEC AWI TR 20322.

[320] Alle im Absatz genannten „benefits“ werden aufgeführt in ISO/IEC TR 24714-1:2008, S. v.

Daten für einen nicht mit dem System vorgesehenen Zweck), *Repudiation* (Abstreiten der Systembenutzung seitens einer registrierten Nutzerin).[321]

Es gibt viele verschiedene Modellierungen für mögliche Bedrohungsszenarien eines biometrischen Systems. Diese dienen auch dazu, im Rahmen des Systemdesigns besser abschätzen zu können, welche Schutzmaßnahmen in einem konkreten Anwendungskontext implementiert werden sollten, welche verzichtbar sind. Maltoni et al., die auch ein eigenes entwickelt haben, nennen das *Attack Point Model* von Bolle, Connell und Ratha,[322] das *Attack Tree Model* von Cukic und Bartlow[323] sowie das *Fishbone Model* von Jain, Ross und Pankanti.[324]

Das *Attack Point Model* wird hier exemplarisch vorgestellt. Analog zur Darstellung in Abbildung 3.6 werden direkt an den einzelnen Komponenten des Biometriesystems oder ihren Schnittstellen grundsätzliche Angriffspunkte ausgemacht. Sie sind wie folgt beschrieben und in vier Gruppen eingeteilt:

- *Manipulation der biometrischen Charakteristik oder der aus ihr generierten Daten am Sensor:* Wenn eine berechtigte Nutzerin etwa von jemand anderem gezwungen wird, ihre biometrische Charakteristik am Sensor zu präsentieren oder sogar der Finger gewaltsam entfernt wird, ist dies eine sogenannte *Coercive Attack*. Die Autoren schlagen vor, solche Angriffe mittels Stresserkennung am Sensor, mit Überwachungskameras oder durch eine Wache von einem Sicherheitsdienst zu vermeiden. Einige dieser Maßnahmen kommen für das Opfer allerdings im konkreten Fall zu spät, helfen erst in einer späteren Ermittlung und schrecken dadurch ab. Ähnlich verhält es sich mit der Lebenderkennung als Gegenmaßnahme bei einer gewaltsamen Amputation eines Körperteils – zwar würde damit ein Datenzugriff verhindert, aber nicht die körperliche Schädigung des Opfers. Die Lebenderkennung dient allerdings auch der Erkennung einer Täuschung (*Masquerade*/*Impersonation*/*Spoofing*) etwa mittels Fake-Fingern aus Gummi oder mit speziellen Klebebeschichtungen auf der Hautoberfläche. Werden hierfür latente Abdrücke von schon erfassten Personen verwendet, spricht man auch von einem *Replay*-Angriff.

  Die Fälschung eines biometrischen Merkmals muss nicht zwangsläufig auf eine genaue Kopie hinauslaufen. In einem Identifikationsszenario kann es auch einfach sinnvoll sein, den Fingerabdruck so zu verändern – durch schmerzhafte Verätzungen, Hautimplantat oder aber Störung oder Manipulation der Datenerfassung am Sensor –, dass er nicht nutzbar ist oder sicher nicht mehr dem gespeicherten ähnelt.

[321] Vgl. Maltoni u. a. 2009, S. 50.

[322] Siehe Bolle u. a. 2004, S. 211 ff.

[323] Siehe Cukic und Bartlow 2005.

[324] Siehe Jain, Ross und Pankanti 2006.

Insgesamt gelten die elektronische oder physische Präsentation von Fake-Fingern als die häufigste Angriffsvariante. Werden sie zudem beim Enrolment in der Datenbank gespeichert, ist dies noch problematischer.

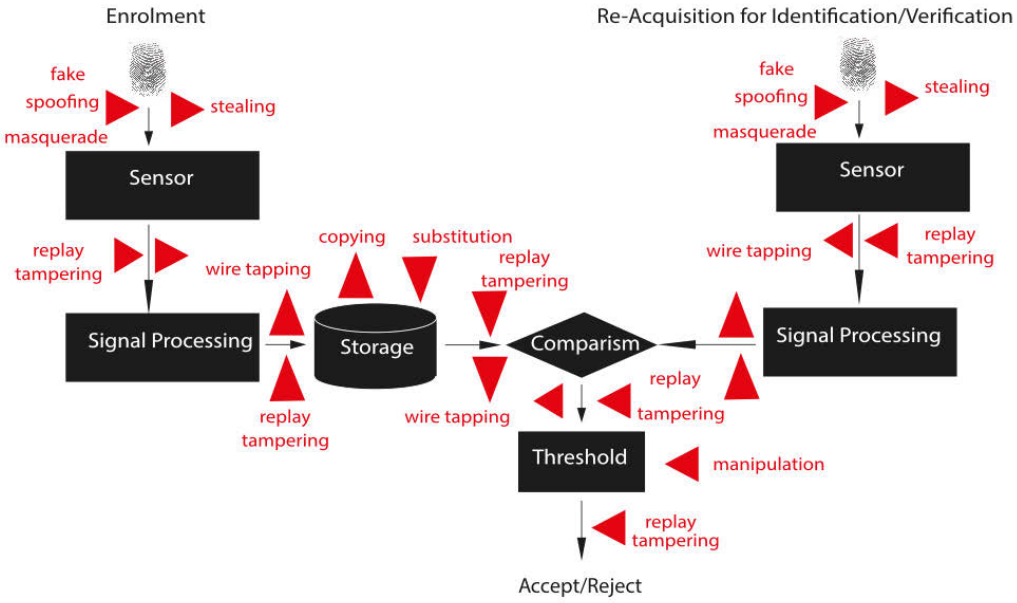


Abbildung 3.6: Mögliche Angriffspunkte in einem biometrischen System. Die an Kevenaar u. a. 2010, S. 47 angelehnte, gestalterisch veränderte und erweiterte Darstellung ähnelt konzeptuell dem *Attack Point Model* von Bolle u. a. 2004, S. 212.

- *Manipulation des Datenflusses zwischen Sensor, Merkmalsextraktion, Vergleich sowie innerhalb der Datenverarbeitung innerhalb dieser Komponenten:* Der Kanal zwischen Sensor und verarbeitendem System ist angreifbar – hier kann ein Replay-Angriff mit bereits digitalisierten Daten erfolgen: Das Einspielen eines falschen Samples, das vielleicht auch an diesem Kanal abgehört (*Wire Tapping*) oder von an anderer Stelle aus zum Beispiel von einer Smartcard gestohlenen Minutien-Templates rekonstruiert wurde. Durch Zeitstempel und Verschlüsselung der Samples und Templates lässt sich solchen Problemen vorbeugen.

  Eine andere Möglichkeit ist eine Signalstörung bei der Übertragung (*Tampering*).

  Zudem können in den Prozess der Merkmalsextraktion künstlich erzeugte Features wie ein trojanisches Pferd eingeschleust werden. Eine andere Variante ist das Einschleusen von Schadcode in das Vergleichsmodul – etwa durch den Austausch bestimmter Programmbibliotheken –, so dass immer ein bestimmter Ähnlichkeitswert für einen oder mehrere spezielle User erzeugt wird.

Gerade bei Systemen, in der beispielsweise das Template auf einer Smartcard, aber das Vergleichsmodul auf einem eigenen Rechensystem installiert sind, ist es ohne entsprechende Vorsichtsmaßnahmen wie Signaturen und Verschlüsselungen leicht, die Übertragung zwischen diesen Modulen abzuhören.

- *Strategien der Umgehung, die Erfassung, Extraktion und Vergleich überspringen:* Dazu gehören die Manipulation der Ausgabe des Vergleichs- oder Entscheidungsmoduls, aber auch die Ausnutzung bestimmter Rechte oder Wartungszugänge für administratives Personal, die immer vorhanden sind, um Reparaturen vorzunehmen, oder das System abzuschalten, um Menschen ohne Finger passieren zu lassen oder ähnliches. Es ist daher nie komplett auszuschließen, dass solch ein Zugang auch betrügerisch oder in geheimer Absprache zur Systemumgehung genutzt wird (*Collusion*).

- *Manipulation der Template-Datenbank:* Auch hier ist natürlich der Übertragungsweg von und zum verteilten Datenbanksystem gefährdet. Ein besonderes Problem ist das Einschleusen eines gefälschten Templates schon beim Enrolment der Daten (*Illegitimate Enrolment*) – dann sind spätere Manipulationen nicht mehr nötig. Dementsprechend müsse das Enrolment auch unter besonderen Sicherheitsvorkehrungen stattfinden. Außerdem können gespeicherte Templates verändert, gelöscht, kopiert und weitergegeben werden. In letzteren Fällen geht es weniger um einen Angriff direkt auf die Applikation, sondern auf die gespeicherten Daten. Die Autoren sprechen daher hier von *Privacy Attacks*. Datendiebstahl ist insofern besonders schwerwiegend, als dass sich hier der gepriesene Vorzug, dass eine biometrische Charakteristik ein Schlüssel ist, den man nicht verlieren und der nicht gestohlen werden könne, in ihr Gegenteil verkehrt. An diesem Punkt setzen die Bemühungen von *Template Protection* sowie aufhebbarer Biometrie (*Cancellable Biometrics*) an.

Die aufgezählten Beispiele sind nicht vollständig,[325] aber bilden eine Herangehensweise der Strukturierung im Vorhinein antizipierbarer „Bedrohungen" eines Fingerabdruckerkennungssystems ab. Chris Roberts vereint diesen und die oben genannten Ansätze in einer praktischen Übersicht, die eine Risikoabschätzung und die Abwägung, welche Sicherheitsmaßnahmen zur Minimierung von Schwachstellen (*Vulnerabilities*) man dementsprechend ergreift, im Rahmen des Systementwurfs erleichtern.[326] Einige spezielle Probleme im Zusammenhang mit Überwindungsfehlern werden in den kommenden Unterkapiteln vertieft.

[325] Zum Beispiel werden in Bolle u. a. 2004, S. 219 ff. noch weitere Angriffe wie die *Hill Climbing Attack*, die *Swamping Attack* oder die *Piggy-Back Attack* sowie mögliche *Brute-Force Attacks* und die erweiterten Möglichkeiten des Angriffs auf Smartcard-gespeicherte Biometrie erläutert.

[326] Siehe Roberts 2007.

3.4.1 Nutzerrollen und Fehler

Überwindungsfehler sind eng an das Nutzerverhalten gebunden. Teilweise überlagern sich allerdings insbesondere beim Begriff *Impostor* verschiedenen Bedeutungen. Roberts benennt diejenigen Nutzerinnen, die die Systemsicherheit bedrohen, „Threat Agents", wenngleich sie gar nicht bewusst oder absichtlich handeln müssen. *Threat Agents* können entweder *Authorised Users*, *Attacker* oder *Impostor* sein.[327] *Authorised Users* verhalten sich unabsichtlich so, dass das System nicht mehr korrekt funktioniert – beispielsweise ein etwas versehentlich falsch konfigurierender Administrator. *Attacker* hingegen wollen das System in irgendeiner Form absichtlich kompromittieren. Ein *Impostor* wiederum gibt sich als eine *andere* autorisierte Nutzerin aus, allerdings nicht zwangsläufig absichtlich.

Wie bereits bei der Erläuterung der Vergleichsfehlerraten deutlich wurde, wird das eigentlich aus dem *Security Engineering* stammende Vokabular *Impostor*/*Genuine Person* im Performanzmetrik-Zusammenhang erstmal ganz unabhängig von Bedrohungen benutzt. Es dient nur der Klassifizierung der Zugehörigkeit von Mustern. Synonym mit *Impostor* werden noch *Incorrect User* (falsche Nutzerin) oder *Illegitimate User* (unzulässige Nutzerin), mit *Genuine Correct User* (richtiger Nutzer) oder *Legitimate User* (zulässiger Nutzer) genutzt. Sie sind im Alltagsgebrauch stark moralisch wertend aufgeladen, aber in Bezug auf den rein technischen Kontext nicht so gemeint: Bei einem richtigen, einem „Correct User" (*richtiger Nutzer*, *echter Nutzer*), produziert der Mustervergleich einen „*genuine match*, because the comparison is between samples from the same user."[328]

Der Begriff des *Betrügers* (*Impostor*) wird synonym zu dem des *falschen Nutzers* („incorrect user") verwendet, also von den Autoren in seiner eigentlichen Härte der Konnotation mit absichtsvollem betrügerischen Verhalten relativiert:

> „In the case of an incorrect user trying to gain access to the laptop, this is known as an *impostor match*. An impostor match is not necessarily from someone deliberately trying to fool the algorithm, as it could be a person who accidentally selected the wrong log-in account. The term ‚impostor' in this context merely refers to the fact that the two matches are not taken from the same biometric characteristic."[329]

Inwieweit es sich also bei einem *Impostor-Match* um einen absichtlichen Betrug handelt und ob das Wort diese Absicht auch real mit transportieren soll, hängt sehr stark vom konkret beschriebenen Kontext ab. In der Regel wird der Begriff im Rahmen von Performanzuntersuchungen unabhängig von der Absicht der betroffenen Personen verwendet und ist dementsprechend ungeeignet und verwirrend.

---

[327] Vgl. ebd., S. 16 f.

[328] Dunstone und Yager 2009, S. 29, Hervorhebung im Original.

[329] Ebd., Hervorhebung im Original.

Ähnlich verhält es sich mit der speziellen auf statistischen Untersuchungen gegründeten Ausdifferenzierung von Nutzerinnen bezüglich ihrer individuellen Performanz in Bezug auf den Abgleich mit zu ihnen gehörenden und nicht zu ihnen gehörenden Templates. Es geht hier nicht um konkrete Betrugsabsichten, sondern eher darum, dass sie einfach aufgrund der individuellen Eigenschaften ihrer biometrischen Charakteristik besonders häufig sehr hohe *Impostor Scores* oder sehr niedrige *Genuine Scores* erreichen. Das heißt, dass sie beim Abgleich mit Templates, die bei ihnen nicht ähnlich sein dürften, hohe Ähnlichkeitswerte erreichen, und bei denen, die ihnen ähnlich sein müssten, da sie von ihnen erzeugt wurden, nur geringe Werte erreichen. Dass es tatsächlich immer Personengruppen gibt, bei denen dies so ist, konnten Doddington et al. Ende der 1990er für Sprecherinnenerkennungsverfahren zeigen. Ihre heute als „Doddington's Zoo"[330] bekannte, daraus abgeleitete Taxonomie impliziert allerdings wieder Wertungen, die den betroffenen Nutzerinnen teilweise Betrugsabsichten unterstellen.
Nutzerinnen lassen sich gemäß Doddington et al. in die Gruppen *Sheeps* (Schafe), *Goats* (Ziegen), *Lambs* (Lämmer) und *Wolves* (Wölfe) aufteilen:

- Schafe: Hierzu gehören die meisten Erfassten. Sie erreichen Ähnlichkeitswerte, die der Mehrheit aller anderen Nutzer entsprechen. Das heißt, ihre Templates passen sehr gut zu anderen Templates, die von ihnen stammen, aber in der Regel nicht so gut zu denen von anderen. Sie haben eine durchweg angemessene Performanz.

- Ziegen: Dies sind Nutzer, die nur niedrige *Genuine Scores* erreichen, also bei Abgleich verschiedener Templates, die von ihnen stammen, nur niedrige Ähnlichkeitswerte erreichen. Bei ihnen ist die Wahrscheinlichkeit recht hoch, häufiger fälschlicherweise nicht erkannt zu werden.

- Lämmer: Wenn Templates anderer Nutzerinnen gegen die von Personen dieser Gruppe abgeglichen werden, werden hohe Ähnlichkeitswerte erreicht. Das bedeutet, dass Lämmer leicht zu imitieren sind, da sie häufiger falsche Übereinstimmungen erreichen.

- Wölfe: Wölfe sind wiederum die Nutzerinnen, die hohe Ähnlichkeitswerte beim Abgleich vor allem mit Lämmern erreichen.

Obwohl es hier nicht um die Absichten oder die realen Handlungsfähigkeiten der betroffenen Personen geht, transportiert die Taxonomie auch eine solche Bedeutung, da sie auf die typischen Charakterzüge abhebt, die den jeweiligen Tieren als Fabelwesen zugeschrieben werden.
Dennoch werden sie scheinbar wertungsfrei als Teil von Performanzbeschreibungen eines biometrischen Systems verwendet. So gehen beispielsweise Dunstone/Yager in

[330] Siehe Doddington u. a. 1998.

ihrem Kapitel »The Biometric Menagerie« ausführlich darauf ein[331] und betrachten den sogenannten *Zoo Plot* als eigenen (um vier weitere Tiergruppen erweiterten) Performanzgraphen (siehe Abbildung 3.7), mit dem sich gut zeigen ließe, welche (Gruppen von) Nutzerinnen mehr oder weniger Systemfehler produzieren.

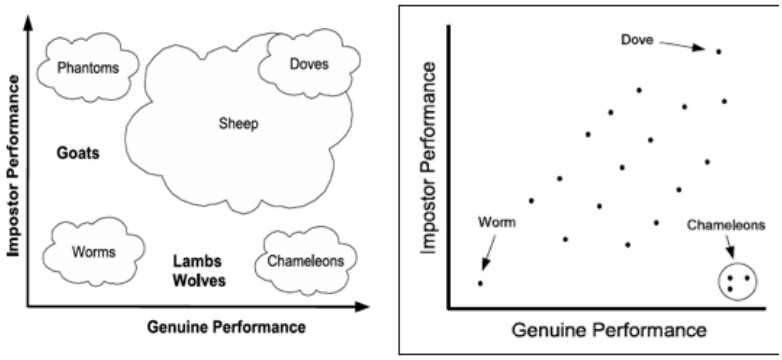


Abbildung 3.7: Beispiel für einen *Zoo Plot*. Er zeigt die Performanz einer Nutzerin, wenn ihr Template gegen zu ihr gehörende abgeglichen wird (*Genuine Performance*, auf der x-Achse), gegen die Performanz abgetragen, wenn ihr Template gegen nicht ihr zugehörige Nutzer-Templates (*Impostor Performance*, auf der y-Achse) abgeglichen wird. Links: Allgemeine Zuordnung der einzelnen Nutzerinnen-Kategorien von „Doddington's Zoo" in einem *Zoo Plot*. Rechts: Konkretes Fallbeispiel für eine mögliche gemessene Verteilung. Beide Abbildungen aus Dunstone und Yager 2009, S. 166, 168, © Springer-Verlag.

3.4.2 Zum Verhältnis von Performanz und Sicherheitsproblemen

Der eben erläuterte *Zoo Plot* ist ein Beispiel für eine Korrelation des Verhaltens betroffener Personen, das in diesem Zusammenhang als potentielles Sicherheitsproblem gesehen wird, und Systemperformanz. Des Weiteren verändern natürlich auch die bereits aufgeführten Angriffe die ideale Systemperformanz. Dennoch werden Tests auf „Security, including vulnerability" in den ISO/IEC-Dokumenten der Reihe 19795 zur Performanzmessung nicht einbezogen.[332]

> „A perfectly accurate biometric system may still be highly vulnerable to attack, as unauthorized users may find alternates ways by which they can be falsely accepted by a system. Compared with the effort expended on determining performance accuracy, significantly less effort has been given to the problem of determining if a presented biometric is real or fake."[333]

[331] Neben Dunstone und Yager 2009, S. 106 f., wird das Konzept als Teil einer Einführung in die Performanzevaluation bei Jain, Flynn und Ross 2008b oder als Teil eines Aufsatzes zur Variabilität der *Receiver Operation Characteristic* (ROC) *Curves* in Wayman 2004 erläutert.

[332] Vgl. ISO/IEC 19795-1:2006, S. vi.

[333] Dunstone und Yager 2009, S. 247.

Die Anstrengungen auch hier zu einheitlichen Qualitätsstandards zu gelangen, haben in den letzten Jahren auch im SC37 erheblich zugenommen. Inzwischen widmen sich offiziell die Dokumente ISO/IEC 29156 mit dem Titel »Guidance for Specifying Performance Requirements to Meet Security and Usability Needs in Applications Using Biometrics« und vor allem das Dokument ISO/IEC 30107 mit dem Titel »Presentation Attack Detection« diesen Fragen.

Letzteres Dokument war nicht zuletzt motiviert durch die zahlreichen Publikationen über erfolgreiche Angriffe auf Biometrie-Systeme. Einer der Ko-Editoren des Entwurfs für ISO/IEC 30107, Rick Lazarick, berichtete auf der *Biometrics Consortium Conference* 2012, dass ein standardisiertes Rahmenwerk, in dem eine klar definierte Taxonomie entwickelt wird und der Fokus auf den sogenannten „Presentation Attacks" liegt, nötig wurde.[334] Eben jene sind auch die Fehler oder Störungen, die wohl am häufigsten in den Medien Niederschlag finden.

3.4.3 Datenschutzgefährdungen

Biometrische Referenzdaten gelten generell als sensible, schützenswerte Daten. Eine sichere Verschlüsselung der Datenbanken und der Kommunikationswege sehen die Metadatenstandards aber lediglich optional vor.[335] Auch in den anderen ISO/IEC-Standards aus der zweiten Hälfte der nuller Jahre herrscht ein Empfehlungscharakter vor. Typisch sind Sätze wie:

> „The decision to maintain a centralized reference template database for verification applications should be done with an assessment of the privacy and security risks should the database be compromised, as well as any associated privacy issues."[336]

Kindt weist darauf hin, dass die Veröffentlichung von »ISO/IEC 24745:2011 Information technology – Security techniques – Biometric information protection« inzwischen konkrete Datenschutzanforderungen und -vorkehrungen zum Schutz von Templates explizit in die Standardisierung mit einbezieht.[337] Dies scheint allerdings momentan auf diesen Bereich beschränkt.

---

[334] Vgl. Lazarick 2012. Schuckers diskutiert die kommerzielle und wissenschaftliche Bedeutung, die eine standardisierte *Presentation Attack Detection* (PAD) hat. Erstmals würden überprüfbare Kriterien und mit *Attack Presentation Classification Error Rate* und *Attack Presentation Match Rate* Metriken eingeführt, die eine systematische Analyse statt lediglich aufsehenerregender Hacks und Einzelfälle ermöglichen. Denn diese zeigten zwar, dass es eine Bedrohungslage gebe, aber „there has been little evidence that widespread fraud based on spoofing has occurred in biometric systems." (Schuckers 2016, S. 2).

[335] Siehe *Abschnitt: Standardisierte Speicher- und Austauschformate* (S. 70).

[336] ISO/IEC TR 24741:2007, S. 12.

[337] Vgl. Kindt 2013, S. 803.

3.5 Begriffs- und erkenntnistheoretische Probleme

Das Biometrie-»Vocabulary« der *Working Group 1* des SC37 von 2012 stellt einen wichtigen Konsens einer zehnjährigen Auseinandersetzung um verbindliche Definitionen von mehr als hundert grundlegenden Termini des Gebiets dar. Biometrie habe als relativ junges Gebiet verschiedene Definitionen jedes einzelnen Begriffs und verschiedene Begriffe für anscheinend gleiche Konzepte, schreibt Rene McIver, der Teil der Gruppe ist.[338] Für die Erstellung des Glossars wurden viele Begriffe und Definitionen aus verschiedenen Quellen zusammengestellt und daraus dann nach den Vorgaben der ISO/IEC für die Harmonisierung von Konzepten und Termini (ISO 860:1996) verbindliche Definitionen synthetisiert.[339]

Das Glossar wird permanent iterativ weiterentwickelt. Die derzeit veröffentlichte Version könnte 2017 die nächste Anpassung erfahren.[340] Die Mitglieder der Arbeitsgruppe erkennen vor allem mit Bezug auf den Wissenschaftssoziologen Thomas S. Kuhn an, dass herrschende wissenschaftliche Paradigmen sich mit der Zeit veränderten, sogar innerhalb einer Disziplin. Historische Entwicklungen, kulturelle und soziale Hintergründe beeinflussten die generellen Konzepte, innerhalb derer und nach denen die Begriffsbezeichnungen der Biometrie in einem Vokabular kategorisiert würden. Eine Terminologieentwicklung erfordere, die speziellen Umstände genau zu kennen, durch die Begriffe von allen anderen eindeutig unterscheidbar sind. So ließe sich eine zeit- und theorieabhängige Wahrheit finden.[341] Neben der sich so ergebenden Abbildung der Begriffsforschung und -bildung hat die Festlegung eines verbindlichen Glossars aber auch pragmatische Gründe. Sowohl die dem sozialen Kontext zugeordnete *Science* als auch die dem kommerziellen zugeordnete *Technology*[342] profitiere nämlich von größerer Übersichtlichkeit bzw. einfacherer Implementierung und der Vermeidung finanziell kostspieliger vertraglicher Missverständnisse.[343]

Zudem zeigt der Wandel des Verständnisses grundlegender Begriffe in der informatischen Biometrie auch deutlich die Verschiebungen des innerfachlichen Diskurses. Ein interessantes Beispiel sind hier die über Zeit und verschiedene Publikationen hinweg unterschiedlichen Begriffsinhalte von *Verifikation* und *Identifikation* – die Hauptverwendungszwecke von Biometrie. Aus Sicht von Wayman et al. spiegelt sich hierin die Ausweitung biometrischer Anwendungsaufgaben wider.[344]

---

[338] Vgl. McIver 2009, S. 158.

[339] Vgl. ebd., S. 159.

[340] Vgl. Wayman, McIver u. a. 2014, S. 7.

[341] Vgl. ebd., S. 2 f.

[342] Vgl. ebd., S. 1.

[343] Vgl. ebd., S. 7.

[344] Vgl. ebd.

Identifikation allein als Erkennung einer Person im landläufigen Sinne ihrer Zuordnung zu einer dem System bekannten Referenz zu sehen oder Verifikation als Bestätigung einer solchen schon postulierten Zuordnung decken nicht alle Anwendungsmöglichkeiten eines Biometriesystems ab. Der Nachweis einer Unterschiedlichkeit mit allen gegebenen Mustern wie zum Beispiel in Watch-Listen oder der Falsifikation einer Verknüpfung zwischen zwei Mustern können ebenfalls Anwendungszwecke sein. Aus Sicht der automatisierten Biometrie mögen dies Neuerungen gewesen sein, doch bereits einer der Wegbereiter der Daktyloskopie, William Herrschel, sah ein Anwendungsgebiet in der Verhinderung betrügerischen Doppelbezugs von Pensionen der britischen Kolonialverwaltung in Indien – das entspricht dem Konzept der negativen Identifikation oder De-Duplikation.

Eine weitere Debatte zur Anwendbarkeit des Begriffs *Identifikation* dreht sich um die Frage, inwieweit er überhaupt impliziert, dass es dem System unbekannte Personen geben darf.[345] Das bedeutet, dass zum einen einige Personen, von denen biometrische Proben aufgenommen werden, nicht im System erfasst sind, und zum anderen, dass vorher nicht klar ist, ob von ihnen bereits Referenzen im System erfasst sind. Es kann hier auch eine leere Kandidatinnenliste geben. Für die negative Identifikationsbehauptung ist es sogar ein Erfolg, wenn die Betroffene Person nicht erfasst ist. Obwohl dieses Szenario, auch als *Open-set Identification* bezeichnet, in der Praxis der Standardfall ist, wurde vor allem *Closed-set Identification* beforscht.[346] In dieser Idealvorstellung wird Identifikation lediglich positiv begriffen. Es können dabei nur im System erfasste Personen geprüft werden – im besten Falle müssten einfach „alle im Universum“ in der Enrolment-Datenbank gespeichert sein, denn eine leere Kandidatinnenliste ist hier nicht möglich.

Inzwischen wird auch eine allzu lockere Verwendung des Begriffs der Identität innerhalb der Biometrie kritisch reflektiert.

3.5.1 Identitätsbegriff

> „Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person.“[347]

Die Biometrie wird in der hier zitierten Definition, die noch nicht allzu alt ist, zur Wissenschaft der Identitätsherstellung einer Person. Das ähnelt der Ansicht von Wayman im Jahr 2000, als er *Biometrics* als „a sub-field of the larger area of human identification science“[348] bezeichnete. Im Vergleich dazu stellt die ISO-Definition in einer von

[345] Vgl. Wayman 2013, S. 17.

[346] Vgl. Maltoni u. a. 2009, S. 15.

[347] Jain, Flynn und Ross 2008b, S. 1.

[348] Wayman 1998, S. 21.

den sechs der Hauptdefinition angehängten Anmerkungen fest, dass die allgemeine Bedeutung von *Biometrics* „counting, measuring and statistical analysis of any kind of data in the biological sciences including the relevant medical sciences“[349] umfasse.

Die Kopplung von Biometrie mit menschlicher Identität aber hat bis heute in der informatischen Biometrie eine sehr nachhaltige Wirkung. Dunstone/Yager führen beispielsweise aus, dass die Identität einer Person nicht im biometrischen Datensatz „steckt“, sondern an diesen gebunden wird. Das bedeutet, dass eine Prüfinstanz, ein menschlicher Zeuge, der ersten Verknüpfung eines biometrischen Datensatzes mit der „korrekten Identität“ beiwohnt. Diese korrekte Identität wird beispielsweise mit einer Geburtsurkunde oder einem Pass als Identitätsbeweis (*Proof of Identity*) hergestellt.

> „Where anyone can self-enroll a biometric with no check or audit, system circumvention is easy, regardless of the strength of the biometric control. This is because there is no way to ensure the correct identity is bound to the enrolled biometric.“[350]

Obwohl also Identität hier durchaus als loses Konzept gesehen wird, schreiben die meisten Autoren – auch Dunstone/Yager – biometrischen Charakteristika und den aus ihnen gewonnen Daten die besondere Eigenschaft zu, dass sie intrinsisch mit dem Konzept von Identität verknüpft seien.[351] Biometrische Daten sind also einerseits in irgendeiner Form innerlich mit unserer Identität verlinkt und andererseits können wir ihnen erst trauen, wenn sie mit dieser korrekt von außen verbunden werden.

Die Sozialwissenschaftlerinnen Vassilis Tsianos und Brigitta Kuster deuten in einer Fußnote ihres Textes zur »Digitalisierung der Europäischen Grenze« die Begriffe *Identifikation* und *Verifikation* als einen kulturellen Komplex, in dem es um das Verhältnis von *einem* Wahren gegenüber möglichem Vielen geht:

> „Diese Unterscheidung [zwischen Identifikation und Verifikation] widerspiegelt die Differenz zwischen Wahrheit und Identität, wie sie im westlichen (Alltags-)Denken etabliert ist. Während die Wahrheit zu erlangen dem Versuch entspricht, die Vermittlung zu liquidieren und auf diese Weise Deckungsgleichheit zu erreichen, ist Identität immer schon konfrontiert mit den Schwierigkeiten des Prozesses, Vielheit abzuziehen. Authentizität wiederum versucht, die Subtraktion der Vielheit der Identität im Singulären anzutreffen.“[352]

Die Vokabular-Arbeitsgruppe des Subcommittee 37 »Biometrics« hat sich einer solchen Auseinandersetzung allerdings eher entzogen und versucht auf den Identitätsbegriff zu verzichten. Man kam stattdessen in Anerkennung der Jahrtausende währenden philosophischen und religiösen Auseinandersetzung um den Identitätsbegriff zu

---

[349] ISO/IEC 2382-37:2017, S. 2, Anmerkung 2 Begriff „biometrics“.

[350] Dunstone und Yager 2009, S. 11.

[351] „Biometric data is special because it is intrinsically linked to our internal concept of identity in a way that other forms of proof of identity, such as passwords and keys, are not.“ (ebd., S. 13).

[352] Kuster und Tsianos 2013, S. 24.

der Ansicht, dass die Identität eines Individuums eine nicht fassbare Eigenschaft ist, die nicht essentiell für die Biometrie sei.[353] Ganz aus dem »Vocabulary« der ISO/IEC verschwunden ist er jedoch nicht. Eine *Identitätsbehauptung* (*Claim of Identity*) sowie *Verdecker einer Identität* (*Identity Concealer*) gibt es fürderhin. Der Bezug zur Identitätsbehauptung ist zwar nur noch eine Anmerkung, aber der Verdecker einer Identität ist noch ein fest definierter Standardbegriff. Eine ganz entschiedene Abwendung vom alten Paradigma einer identitätsfeststellenden Biometrie gab es dann wohl doch nicht. Dies dürfte vor allem dem Anspruch der Gruppe geschuldet sein, im größtmöglichen Ausmaß bisher gebräuchliche Begriffsnutzungen zu berücksichtigen.[354] Auch mit ‚alten' Begriffen war zudem den Kennerinnen der Materie lange klar:

> „Biometric authentication has the capacity to connect a person through the measured characteristics to an identity as previously enrolled in a database. This technology cannot link a person to any identity outside the system."[355]

Die Identifizierung oder die Verifikation beziehen lediglich sich auf in dem System abgelegte spezifische Daten von bestimmten messbaren Merkmalen eines Menschen. Es ist daher zu weit gegriffen, gleich von der Herstellung einer gesamten Identität zu sprechen. Denn dieser Begriff impliziert weit mehr als bloß die annähernde Deckungsgleichheit einzelner Charakteristika. Insofern ist auch der Ausdruck „körperliche Quelle einer […] biometrischen Referenz" weniger irreführend als „an identity as previously enrolled in a database".

3.5.2 Repräsentationsprobleme

> „The representation issue constitutes the essence of fingerprint recognition system design and has far-reaching implications on the matching modules."[356]

Das digitale Fingerabbild soll einen Finger praxistauglich und unverwechselbar repräsentieren – Maltoni et al. sprechen von den Anforderungen der *Suitability* bzw. *Saliency* einer Fingerabdruckrepräsentation.[357] Dies impliziert zweierlei: Erstens wird ein Original vorausgesetzt, das, zweitens, durch den Abbildungsprozess eine Änderung erfährt, die zu einer Fehlrepräsentation desselben führen kann. Das Originalmuster wird bereits bei der sensorischen Erfassung verändert und mindert demnach dessen Wiedergabetreue. Diese Abweichung vom angenommenen Original zu messen und von der intrinsischen Qualität des Fingers oder seinem körperlichen Zustand

[353] Vgl. Wayman, McIver u. a. 2014, S. 4.

[354] Vgl. ebd.

[355] Wayman 1998, S. 22. Der Begriff *Biometric Authentication* wird hier noch synonym zu *Biometric Recognition* benutzt.

[356] Maltoni u. a. 2009, S. 38.

[357] Vgl. ebd., S. 39.

zu entkoppeln stellt ein schwieriges Problem dar.[358] Dieses Problem wird auch mit den Begriffen der *Within-Individual Variation* oder *Intra-Class Variation* und *Between-Individual Variation* oder *Inter-Class Variation* charakterisiert. Eine gute Repräsentation zu finden bedeutet im Kontext der Mustererkennung die Bestimmung eines Messraumes, in dem Fingerabdruckbilder, die zum selben Finger gehören, eine geringe Intra-Klassen-Variation aufweisen, und Bilder, die zu verschiedenen Fingern gehören, eine hohe Inter-Klassen-Variation.[359]

Die Festlegung dieses Messraums ist ein Akt der interpretativen Herstellung einer Eindeutigkeit des gemessenen Merkmals, dem mit diesem Vorgang eine spezifische Originalität zugeschrieben wird. Es mag variieren, aber es darf nur in einem Rahmen variieren, der Individualität garantieren muss. Einerseits ist für den biometrischen Prozess explizit klar, dass die Messapparatur richtig konstruiert sein muss, um die Unverwechselbarkeit des gemessenen Bildes abzusichern, andererseits ist genau die Annahme der Existenz dieser Unverwechselbarkeit, die nicht erst hergestellt werden muss, eine Bedingung der Möglichkeit von funktionierender Biometrie.

Dieser paradoxe Umstand ist den Biometrie-Forschenden in der Regel bewusst:

> „[…] the fundamental requirement of any biometric recognition system is a human trait having several desirable properties like universality, distinctiveness, permanence, collectability, acceptability, and resistance to circumvention. However, a human characteristic that possesses all these properties has not yet been identified. As a result, none of the existing biometric systems provide perfect recognition and there is a scope for improving the performance of these systems“[360]

Als Konsequenz werden Strategien wie *Biometric Fusion*/*Multimodal Biometrics*/*Multibiometrics* verfolgt oder als noch weniger stabil geltende Informationen über eine Person wie „gender, ethnicity, age, height, weight and eye color“[361] hinzugezogen. Hiermit können dann die biometrischen Daten ergänzt werden. So lässt sich dem gewünschten Effekt näherkommen, eine wirklich dauerhaft zuverlässige Identifizierung zu ermöglichen.

3.6 Fehleruntersuchungen jenseits der Informatik

Da biometrische Technik insbesondere auf hoheitlicher Ebene eine hoch umstrittene Kontrolltechnologie ist, gibt es jenseits der Informatik viele Untersuchungen, Studien und Analysen, die Biometrie im Ergebnis als gesellschaftlich nicht sinnvoll teilweise oder komplett ablehnen oder als Teil einer bestimmten Ideologie kritisieren.

---

[358] Vgl. ebd., S. 72 f.

[359] Vgl. ebd., S. 38 f.

[360] Jain, Dass und Nandakumar 2004, S. 1.

[361] Ebd.

Die vergleichsweise geringe Zahl an Publikationen in Sozial-, Rechts- und Geschichtswissenschaft sowie in interdisziplinären Forschungen, die mehrere Fachrichtungen dieser Gebiete und manchmal auch die Informatik selbst einbeziehen, setzt sich speziell mit der (Kriminal-)Geschichte des Fingerabdrucks, Ethik-, Akzeptanz- und Nutzungsforschung und den Themen Biopolitik, Governance, speziell Pass- und Grenzpolitik auseinander. Gerade im Bereich der Migrationsforschung gibt es zahlreiche Untersuchungen zu einzelnen Biometrie-Projekten. Ein Beispiel ist das eingangs dieser Arbeit genannte Eurodac-System, das von einigen Autoren sowohl in Bezug auf die Interessen beteiligter Akteure sowie hinsichtlich der überwachungspolitischen Implikationen eingehend analysiert wurde.[362]

In den letzten Jahrzehnten sind vor allem Untersuchungen erschienen, die die mit der massenhaften Implementierung biometrischer Identifizierungstechniken einhergehenden Probleme und Konflikte in ihrem sozio-technischen Zusammenhang analysieren.[363]

Eine breite Auswahl von Biometrie-Projekten verschiedener Länder wird erstmalig unter gemeinsamen Fragestellungen in dem von Colin J. Bennett und David Lyon herausgegebenen Sammelband »Playing the Identity Card« untersucht.[364] Hier werden Legitimationsstrategien und politische Reaktionen auf die Einführung biometrischer Pässe in verschiedenen Staaten dargestellt.

Eine sozialhistorische und philosophische Untersuchung der Rolle der Fingerabdruckidentifizierung in der Entstehung der Biometrie hat Daniel Meßner am Institut für Geschichte der Universität Wien im Rahmen seiner Dissertation »Die Erfindung der Biometrie – Identifizierungstechniken und ihre Anwendungen, 1870–1914« vorgenommen.[365]

3.7 Bildungsprojekte zur Biometrie und die Rolle der Fehler

Im Bildungsbereich gibt es eine wachsende Zahl an spezialisierten Kursen, die weitestgehend informatische Schwerpunkte haben. Mit der breitflächigen Einführung biometrischer Technologien ist ein wachsender Bedarf an speziell ausgebildeten „biometric professionals“ wie Front-End-Operatorinnen, Projektmanagerinnen und System-

[362] Siehe Ploeg 1999, Aus 2006 oder Kuster und Tsianos 2013.

[363] Im deutschen, europäischen und anglo-amerikanischen Kontext gehören dazu beispielsweise größere Studien wie Petermann und Sauter 2002, Petermann, Scherz und Sauter 2003, G. Hornung 2005, Maghiros u. a. 2005, Goldstein u. a. 2008, Pato und Millett 2010, Artikel-29-Datenschutzgruppe 2012 oder Lyon 2013 sowie am aktuellsten Kindt 2013.

[364] Bennett und Lyon 2008.

[365] Siehe Meßner 2015.

entwicklerinnen konstatiert worden, um Vertrauen und Integrität der Prozesse und Systeme herzustellen und zu garantieren.[366]

Ausbildungen, Weiterbildungen, Unterrichtsprojekte rund um informatische Biometrie gibt es auf dieser Ebene daher inzwischen in großer Zahl, da die zugehörigen Techniken weltweit immer gängiger eingesetzt werden.

Schon für die Daktyloskopie als Kriminaltechnik wurde über Jahrzehnte hinweg bereits ein weitverzweigtes Zertifizierungs- und Ausbildungssystem etabliert.[367] Die hier entstandene Community hat ihre Ausbildungsprogramme für den forensischen Bereich inzwischen umfassend für den Einsatz automatisierter Fingerabdruckerkennungssysteme erweitert.

Die große Lücke in Forschung und Ausbildung besteht in einer systematischen, fehler- und problemorientierten Herangehensweise, die die sozialen, politischen und geschichtlichen Dimensionen in die Konstruktion der technischen Fehler integriert und verständliche Vermittlungskonzepte anbietet. Die grundlegenden wissenschaftsgeschichtlichen erkenntnis- und diskurstheoretischen Reflexionen und konstruktivistischen Herangehensweisen sind momentan in den Sozial- und Kulturwissenschaften verortet, dort vor allem in den *Surveillance, Border* oder *Science and Technology Studies*.

Neben den institutionell organisierten Bildungsprogrammen gibt es im Bereich der Biometrie immer wieder interessante Selbstlernansätze. Einer davon soll im Folgenden etwas detaillierter vorgestellt werden, da er einen Hands-On-Lernansatz auf der Ebene des Programmierens darstellt und auf das Programm SourceAFIS, das dabei entstanden ist, im Rahmen des in dieser Arbeit entwickelten Lernprojekts zurückgekommen werden soll.

3.7.1 Learning By Coding: Open-Source-Fingerabdruckerkennung

Die in diesem Kapitel kurz vorgestellte quelloffene Fingerabdruckerkennungssoftware *SourceAFIS* ist in zweierlei Hinsicht didaktisch interessant. Zum einen ist sie eines der wenigen Programmpakete, das im Rahmen eines Bildungsprojekts für eine Analyse des Quellcodes geeignet wäre. Zum anderen ist sie selbst Resultat eines Selbstlernprozesses, wie im Folgenden näher ausgeführt wird, und ist damit auch Fallbeispiel und Inspiration für ein autodidaktisches Lernen durch Softwareentwicklung.

---

[366] BEST Network 2010, S. 4, die Publikation enthält eine Liste von 25 kommerziellen oder akademischen Kursen weltweit, darunter etwa den internationalen Online-Kurs *IEEE Certified Biometric Professional* oder den zwischen 15 Monaten und fünf Jahren angelegten Master of Science in *Biometrics Identification Systems* verschiedener Hochschulen aus Großbritannien und Deutschland.

[367] Vgl. Cole 2001, S. 194 ff. sowie ebd., S. 264 ff. Eine wichtige Institution ist hier die 1915 gegründete *International Association for Identification* (IAI) und ihre seit 1995 existierende Arbeitsgruppe SWGFAST.

> „SourceAFIS is a software library for human fingerprint recognition. It can compare two fingerprints 1:1 or search a large database for matching fingerprint[s]. It takes raw fingerprint images on input and produces matching score on output.“[368]

Der Entwickler Robert Važan beschreibt auf seiner Projekt-Webseite, dass er die Implementierung von SourceAFIS nach seinem Ausscheiden bei der Firma *Innovatrics* im Dezember 2009 begonnen habe, um herauszufinden, wie der Mustervergleich in einer Biometrie-Software programmiert ist. Alle ihre Komponenten habe er in seiner zweieinhalbjährigen Arbeit für das Unternehmen genau kennenlernen dürfen, nur diese eine nicht. Die Firma hielt den Quellcode dieses „Kernalgorithmus“ ihrer Software, wie Važan ihn nennt, vor den Mitarbeiterinnen geheim. Gerade dieser Umstand war für ihn der Ansporn, einen eigenen zu entwerfen, um zu verstehen, wie ein solcher Mustervergleich so schnell sein könne und wie er mit Schwankungen in den Vergleichsergebnissen fertig würde.[369]

Er konnte aus dem Studium anderer vorhandener Open-Source-Projekte, vielen Webressourcen und seiner in der Firma gesammelten Erfahrung schließlich eine Applikation produzieren, die in kleinen und mittleren Unternehmen mit bis zu 1000 erfassten Personen oder im akademischen Kontext zu Lehr- und Forschungszwecken genutzt wird. Mitte 2010 ließ der Entwickler seine Vergleichsalgorithmen bei dem offiziellen, in der Biometrie-Community als unabhängig geltenden *Fingerprint Verification Competition* (FVC) testen. Dort schnitt das Programm zwar mit vergleichsweise schwachen Fehlerraten ab.[370] Allerdings ist SourceAFIS eine der wenigen frei verfügbaren und nutzbaren, relativ zuverlässig funktionierenden und überhaupt derartig getesteten Softwares jenseits des kommerziellen Bereichs. Beliebige Datenbanken für Performanztests lassen sich daran anbinden. In diesem Zusammenhang ist ein weiteres Software-Projekt der kubanisch-mexikanischen Informatiker Loyola-González, Medina-Pérez, Gutierrez-Rodríguez und García-Borroto interessant, das die Algorithmen von SourceAFIS und anderen Fingerabdruckerkennungsprogrammen in einem quelloffenen, explizit für Lernzwecke und Studienprojekte gedachten Evaluationswerkzeug integriert, das stark am *FVC-onGoing Web System* orientiert ist: »A Framework in C# for Fingerprint Verification«.[371]

---

[368] Kurzbeschreibung des Projekts auf http://sourceforge.net/projects/sourceafis, letzter Abruf: 28.7.2017.

[369] Vgl. Važan 2012a.

[370] Die Korrektheit des Algorithmus wird in diesem Test mit der *Equal Error Rate* (Gleichfehlerrate) angegeben. In dem Wettbewerb erreichte die Software 3,65 % – für Važan ein Erfolg. Der Wert besagt, dass dies die niedrigstmögliche durchschnittliche Rate falscher Vergleichsergebnisse ist. Zum Hintergrund des Testlaufs *FVC-onGoing* vgl. Dorizzi u. a. 2009. Zu den Testergebnissen: https://biolab.csr.unibo.it/FvcOnGoing/UI/Form/AlgResult.aspx?algId=777, letzter Abruf: 28.7.2017.

[371] Siehe Loyola-González u. a. 2015. In einem weiteren Artikel geben die Autoren eine Übersicht über Einschränkungen von acht im Netz verfügbaren Fingerabdruckerkennungswerkzeugen, von denen

SourceAFIS, das die Entwickler unter anderen Programmen sehr inspiriert hat, ist demgegenüber noch stärker autodidaktisch motiviert. Važan hat jenseits im Web vorhandener Ressourcen nach eigener Aussage nie auf klassische biometrische Grundlagenliteratur zum Erlernen der Funktionalität zurückgegriffen.[372] Er betont daher, dass er nicht die Absicht habe, eine Dokumentation zu verfassen, sondern dass Forschungspapiere sowie Bücher über Fingerabdruckerkennung genutzt werden sollten, um über das Fachgebiet zu lernen. SourceAFIS sei kein Forschungsprojekt, sondern eine Implementierung vieler gut bekannter Techniken. Es gebe keinen Grund für eine Wiederholung des Wissens auf seinem Blog oder irgendwo sonst.[373] Im Diskussionsforum zu SourceAFIS gibt es hin und wieder in ähnliche Richtung abzielende Fragen, die Važan in der Regel dann doch ausführlicher beantwortet und die ebenfalls hilfreiche Hinweise bieten, um mehr über die Software und seine autodidaktische Herangehensweise bei der Entwicklung zu lernen. Ende Mai 2013 schreibt beispielsweise eine Nutzerin, die angibt, ihre Kenntnisse über Biometrie erweitern und ihre Programmierfähigkeiten verbessern zu wollen, dass sie jetzt begonnen habe, über Fingerabdruckidentifizierung zu lesen und als erste wichtige Themen nun „Image enhancement, with Segmentation, Normalization, Orientation and frequency, Binarization and Thinning“ anzugehen seien. Auf ihre Bitte, ihr zu sagen, ob dies die richtige Herangehensweise sei, antwortet der Entwickler:

> „Since biometrics is an area with tons of existing research and products, both commercial and opensource, your first step before writing a single line of code is to learn from others. Read about standard algorithms on the web and in books, go through presentations for existing implementations (both NIST and FR-SDK have such presentations), read source code and identify standard algorithms in it. Then build your prototype (no optimizations, no API, no tuning) and benchmark it against sample database. Log output at each stage and check it visually. You don't want to do more than a simple prototype given your stated goal of learning about biometrics.“[374]

Nicht nur im Kontext eines Software-Entwicklungsprozesses sind visuelle Ausgaben extrem hilfreich. Važan erklärt im oben zitierten Blogeintrag, dass er den Eindruck habe, ein beträchtlicher Teil von Endanwenderinnen würde ein *Graphical User Interface* (GUI) schätzen. Daher habe er vor, die allgemeine *User Experience* zu verbessern. Sein Fokus aber lege auf der Performanz, denn dies sei im Gegensatz zu trivialen

nur *SourceAFIS*, die *NIST Biometric Image Software* und *BiometricSDK* auch den Code für Vergleichs- und Merkmalsextraktionsalgorithmen zur Verfügung stellen, vgl. Medina-Pérez u. a. 2014, S. 133.

[372] Vgl. Važan 2014.

[373] Vgl. Važan 2012b.

[374] Važan 2013a. An anderen Stellen verweist er auf die genannten Dokumente: Hierzu gehören die *Preprocessing*-, *Feature-Extraction*- und *Matching*-Algorithmen des *Fingerprint SDK* (FR-SDK), siehe O. Ostap o. J. bzw. V. Ostap o. J., sowie die Dokumentation der Extraktions- und Vergleichsalgorithmen der *NIST Biometric Image Software*, siehe C. I. Watson u. a. 2007b bzw. C. I. Watson u. a. 2007a.

hübschen Anwendungen rund um die Kernbibliothek der harte Teil, den er beitragen könne.[375] Dementsprechend gibt Važan keine allgemeinverständlichen Anleitungen, wie die herunterladbaren Beispielapplikationen installiert oder genutzt werden können, sondern lediglich eine an Entwicklerinnen gerichtete Dokumentation zur Einbindung der API in eigene Software.[376] Die eher abfällige Haltung gegenüber der trivialen Implementierbarkeit eines geeigneten *User Interface* entspricht der jahrzehntelangen Ignoranz oder Geringschätzung eines nutzerzentrierten Designs in informatischer Softwareentwicklung, das von einer Kernentwicklung abgetrennt schien und für Usability maximal auf die Erfahrungen der Entwickler rekurrierte.[377] Gleichzeitig zeigt der weiter oben zitierte Hinweis zum Vorgehen beim Erlernen der nötigen Fähigkeiten zur Implementierung eines Biometrie-Softwaresystems ganz klar, wie notwendig gerade bei der Entwicklung auch grafische Kontrollausgaben sind.

SourceAFIS, Version 1.7, ist in C#/.NET und experimentell in Java programmiert. Alle mit grafischen Benutzungsschnittstellen umgesetzten Teilanwendungen laufen lediglich mit dem Windows-basierten *.NET Framework*. Das Programm ist in die folgenden sechs Namensräume aufgeteilt, die in Abbildung 3.8 zu sehen sind:

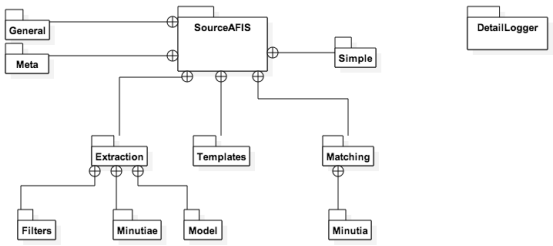


Abbildung 3.8: Paketstruktur der Software SourceAFIS, Version 1.7.

- SourceAFIS.Simple – erzeugt das Objekt *AfisEngine* mit seinen Methoden *Extract*, *Verify* und *Identify* und den Zugriffsmethoden (C#-*Properties*) für die Anpassung der Konstanten *Dpi* (Auflösung des Eingabe-Samples), *Threshold* (Höhe des Ähnlichkeitswerts, ab dem verglichene Templates als übereinstimmend gelten) und *MinMatches* (Anzahl der Finger, die bei einer Person übereinstimmen müssen, um die Person als Quelle eines Templates einzustufen); der Namensraum stellt die API für SourceAFIS bereit, zu der neben der *AfisEngine* die Klassen *Person* und *Fingerprint* gehören, mittels derer ein aufgenommener Fingerabdruck einer Person zugeordnet wird,

[375] Vgl. Važan 2012b.

[376] Siehe Važan 2013b.

[377] Vgl. Bath 2009, S. 223.

- SourceAFIS.General – stellt diverse Datentypen für die Bild- und Vektorverarbeitung bereit, enthält fundamentale mathematische und geometrische Funktionen sowie Ausnahmebehandlungs- und Protokolliermethoden,

- SourceAFIS.Meta – bietet weitere Datenstrukturen und eine Auflösungsanpassung für die eingelesenen Bilder,

- SourceAFIS.Extraction – zentrale Biometrie-System-Komponente, bei der aus dem im JPEG-, PNG-, TIFF-, GIF- oder BMP-Format eingelesenen Fingerbild nach zahlreichen Filter- und Anpassungsmethoden das *Template* extrahiert wird, das in diesem Falle aus numerischen Repräsentationen der die Fingerabdrücke beschreibenden Merkmale besteht; das Template ist schneller verarbeitbar und wesentlich kleiner als das ursprüngliche Bild,

- SourceAFIS.Templates – zentrale Biometrie-System-Komponente, die die Klassen enthält, deren Objekte zur Template-Erstellung und -speicherung nötig sind,

- SourceAFIS.Matching – zentrale Biometrie-System-Komponente, die den durch die og. Methoden *Verify* oder *Identify* ausgelösten Vergleich implementiert.

3.8 Fazit

Es ist an mehreren Stellen deutlich geworden, dass die Unzulänglichkeiten der Biometrie in der Fachliteratur nicht bezweifelt, sondern sowohl in Bezug auf die Fehlerraten in der Mustererkennung als auch die Überwindungssicherheit einen wichtigen Platz einnehmen. Im Gegenteil: Die Einschränkung, dass es weder ein komplett sicheres noch ein komplett fehlerfreies System gibt, ist nahezu obligatorisch. Gleichzeitig ist der Fokus der Fehlerforschung auf bereits innerhalb der Informatik stark normierte Fehlerbereiche – System-, Konformanz- und spezifische Arten von Überwindungsfehlern hochproblematisch. Zwar gibt es im Rahmen der Auseinandersetzung der Anpassung der Systeme an sich ändernde Körper- und Umweltbedingungen, die die Funktionalität und die Interaktion des Nutzers mit dem System möglichst wenig beeinträchtigen sollen, auch Berührungspunkte zu dem formal weniger gut fassbaren Bereich des Fehlers. Aber im Großen und Ganzen bleibt diese Forschung randständig, da sie nicht als originär informatisch gilt.

Der analytische Ansatzpunkt der Gliederung der Fehler in fünf Fehlergruppen suggeriert allerdings ebenfalls eine gewisse Nebenläufigkeit aller dieser Kategorien, so dass sich die stärker dem gesellschaftlichen oder begriffstheoretischen Kontext zugeordneten Gruppen scheinbar deutlich von informatischen Fragen abgrenzen lassen. Es geht allerdings darum zu erkennen, dass die stark abstrahierten Fehlergruppen von den äußeren gesellschaftlichen Bedingungen abhängen, diese reduziert modellieren

und viele auf gesellschaftswissenschaftlicher Ebene theoretisch noch erfassbaren Fehler damit ausklammern und fälschlicherweise ignorieren.

Kommen wir in diesem Zusammenhang nochmal zurück auf die transdisziplinäre Rahmentheorie des Fehlers, die Weingardt aufgestellt hat.[378] Er bietet hierfür eine Veranschaulichung (Abbildung 3.9) an, die kurz erläutert und in Verbindung mit der weiteren Analyse gebracht wird.

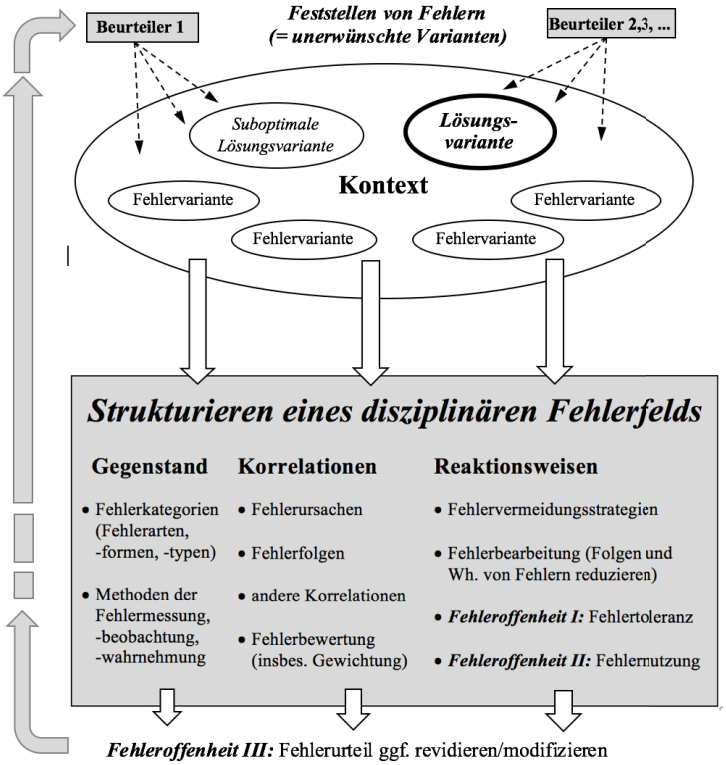


Abbildung 3.9: „Das Strukturieren von Fehlerbereichen als ein zirkulärer Prozess zwischen der Rahmentheorie und disziplinären Fehlertheorien". Abbildung von Weingardt 2004, S. 297.

Das disziplinäre Fehlerfeld ist Teil eines innerdisziplinären „Erkenntnisinteresse[s], das auf Fehlerphänomene und -ursachen ausgerichtet" ist, das Fehlerphänomene typisiert und Ursachen, Auslöser, Bedingungen und Vermeidungsstrategien vorschlägt.[379] Die Rahmentheorie des Fehlers versucht nun in einem größeren Rahmen abzustecken, welche Prozeduren die Entstehung der Typologien begleiten:

[378] Siehe bereits *Kapitel 2.5.*

[379] Weingardt 2004, S. 296.

„- Wie kommt das Urteil, welches ein Fehler sei, zustande und wie wird es revidiert?
- Welchen Zusammenhang zeigen Fehlervermeidung und Fehleroffenheit in den Prozessen dynamisch-komplexer Gegenstandsbereiche bzw. Fehlerkontexte?
- Welcher produktive Nutzen kann von Fehlern ausgehen?“[380]

Der Zusammenhang zwischen einem innerdisziplinären Fehlerfeld und dem dessen Strukturierung beeinflussendem Kontext ist ein Fehlerparadoxon, das einem sinnvollen Umgang mit Fehlern zugrundeliegt. Dieses besagt, das der „Kardinalfehler, ein nachhaltig verfolgtes Interesse nicht zu erreichen am ehesten [vermieden wird], wenn Fehleroffenheit hergestellt wird“. Das heißt, dass „durch bewusst geschaffene Strukturen unerwartete […] Fehler geschehen dürfen“ (*Fehlertoleranz*), „durch einen produktiven Umgang mit Fehlern, die sich ereignen, diese für das Erreichen der Lösungsvariante genutzt werden können“ (*Fehlernutzung*) und dass „eine Offenheit dafür [besteht], dass sich durch die in Prozessen gewandelten Kontexte die angestrebte Lösungsvariante unerwartet als Fehler und eine bislang als ungünstig und unerwünscht beurteilte Fehlervariante als Lösung darstellen kann“ (Fehlerneubeurteilung).[381] Insbesondere die letztgenannte Ebene des Fehlerumgangs erlaubt eine grundsätzliche Infragestellung des gesamten Anwendungs- und Fehlerfeldes und vermeidet eine zu starke Fixierung allein auf Verbesserung des nicht mehr änderbaren Systems. Wichtig hierfür ist die Einbeziehung der den Kontext eines Systems beurteilenden Akteure und die grundlegende prozedurale Sicht einer Fehlertheorie. Die Dynamik der Fehlertypologien auch in der Biometrie ist bereits sichtbar geworden und wird im anschließenden Diskurskapitel noch stärker herausgearbeitet.

Das Systemdesign in der Biometrie, aber auch allgemein in der Informatik bildet in gewissem Maße mittels eines anforderungsgebundenen Entwurfs, der in agilen Theorien auch durchaus in permanenter Dynamik verbleibt, einen ähnlichen Fehlerumgang ab. Allerdings gibt es mit dem Kunden in der Regel nur einen einbezogenen beurteilenden Akteur. Selbst wenn etwa im Rahmen eines nutzerorientierten Designs auch andere Nutzergruppen als allein die Kunden berücksichtigt werden, bilden weder Systementwurfsmodelle noch Weingardts Modell die Hierarchisierung und Machtbezüge verschiedener mit dem System in Interaktion stehender Akteure ab.

Die vorliegende Arbeit setzt u. a. an diesem Punkt an. In Bezug auf Weingardts Modell werden im anschließenden Kapitel genauer der Kontext, das Sagbarkeitsfeld rund um die Fehler der Fingerabdruckerkennungstechnik und die verschiedenen beurteilenden Akteure analysiert. Es geht allerdings noch stärker um eine integrierte Betrachtung des disziplinären Fehlerfeldes als Teil des Kontexts, der hier Fehlerdiskurs genannt wird. Die zu schließende Forschungslücke besteht also zum einen darin, eine integrative Betrachtung eines Fehlerdiskurses innerhalb eines konkreten Forschungsgebiets der

[380] Ebd.

[381] Ebd.

Informatik und die Beschreibung von dessen Struktur zu ermöglichen, in dem Bezüge zu den Analysen in Sozialwissenschaften, Technikgeschichte und Philosophie hergestellt werden. Dies soll über die eher parallel und nicht in Dialog gebrachten Einzelperspektiven der Kompendien interdisziplinärer Tagungen hinausgehen. Zum anderen wird versucht, die spezifische Rolle und Funktion des Fehlers in Bezug auf den sozialen Zweck der Fingerabdruckerkennungstechnik herauszuarbeiten: Wie verhalten sich die Fehler zur Lösung des „Identifizierungsproblems"? Worin besteht dieses Problem eigentlich? Warum und in welcher Hinsicht werden welche Fehler in Bezug auf den Nutzen der Technik für die Lösung des Problems als zu vernachlässigend angesehen?

Die grundsätzliche Befragung der begrifflichen Implikationen, Menschen- und Gesellschaftskonzepte werden hierbei einbezogen und nicht aufgrund ihrer Komplexität ausgeklammert.

Diese Herangehensweise soll zudem in eine andere, fehlerorientierte Vermittlungsstrategie übertragen werden. Während die informatischen Spezialisierungen in der Biometrie vorrangig vor allem auf die Vermittlung der positivistisch gedachten technischen Konzepte ausgelegt sind, bei denen prinzipiell die Sinnhaftigkeit und Funktionstüchtigkeit des Systems nicht gleich in Frage gestellt wird, ist der didaktische Ansatz hier ein von Anfang an kritischer. Es wird gleich vom gesellschaftlichen und normativen Zweck der Überwachungstechnik und ihrer Interessengebundenheit ausgegangen, indem diskursanalytisch gearbeitet wird. Zudem wird von Anfang an auf dieser Ebene, aber auch auf technisch-konstruktiver Ebene nach den Fehlern der Technik gefragt – es ist zwingend, dass man dafür versteht, wie sie überhaupt funktionieren soll –, doch dies soll experimentell und kontrovers erschlossen werden in der Hoffnung, genau die Fehleroffenheit von Beginn an herzustellen, die nötig ist, um einer derart gesellschaftsrelevanten Technik mündig begegnen zu können.

4 Diskurse um Fehler in Fingerabdruckerkennungssystemen

In diesem Kapitel soll es um das diskursive Spannungsfeld gehen, das daraus entsteht, dass die Biometrie eine gesellschaftliche Kontrolltechnologie ist, die sich einem Rechtfertigungsdruck ausgesetzt sieht. Die Akzeptanz der Vermessung einer biometrischen Charakteristik seitens eines Betroffenen ist ein zentrales Design-Kriterium,[382] wenngleich sie in vielen Anwendungsszenarien gar nicht berücksichtigt werden kann. Dies ist der Fall, wenn betroffene Personen aufgrund gesetzlicher Regelungen oder Firmenpolitiken ein biometrisches System benutzen *müssen*. Dementsprechend wird dieses Kriterium manchmal etwas aufgeweicht wie zum Beispiel in diesem wissenschaftlichen Einführungstext zur Biometrie:

> „*Acceptability*: The particular user population and the public in general should have no (strong) objections to the measuring/collection of the biometric."[383]

Im Rahmen ihrer Studie zur sozialen Akzeptanz biometrischer Fingerabdruckerkennung sind die Soziologinnen Susanne Krasmann und Sylvia Kühne in ihren Interviews zur Alltagswahrnehmung von Biometrie bei den Interviewten auf zwei immer wieder auftauchende Motive gestoßen, die widersprüchlich erscheinen. Zum einen gibt es die Angst, die Kontrolle über das digitalisierte Fingerbild zu verlieren: „[…] a fear of loss: as soon as a fingerprint is submitted to a governmental authority, it may obtain a life of its own."[384] Zum anderen wird der Fingerabdruck als etwas Eindeutiges und Objektives gesehen in dem Sinne, dass er eine eigene Wahrheit über etwas Geschehenes transportiert, die unabhängig von dem ist, was real passiert ist:

> „There is no doubt that once a fingerprint is found somewhere as a left trace, it will speak the truth. That *my* fingerprint is at issue, proving that I was *there*, i.e. at the crime scene in question, will be undeniable. The fingerprint verifies ‚that it's me'. The fear of unnoticeably being profiled and (falsely) identified […] rests upon a belief in the objectivity of the fingerprint."[385]

Krasmann und Kühne zeigen die performativen Effekte auf, die irrationale Vorstellungen und herrschender Überwachungsdiskurs zur Verfestigung dieses Glaubens in die Objektivität des Fingerabdrucks beitragen. Diese sei zu einem Mythos in Roland Barthes' Sinne geworden, also ein Signifikant, ein Bezeichnendes in fiktionalen Narra-

[382] Siehe *Kapitel 3.1 Fehler und Biometriesystem-Design* (S. 83).

[383] Bolle u. a. 2004, S. 6.

[384] Krasmann und Kühne 2014, S. 1.

[385] Ebd.

tiven, das ein Eigenleben entwickle.[386] Ein Mythos, der sich, wie der Historiker Simon Cole in seinen Publikationen mehrfach herausgearbeitet hat, auch dadurch festgesetzt hat, dass er innerhalb der Kriminalistik über Jahrzehnte als wahr behauptet wurde, ohne wirklich jemals wissenschaftlich belegt worden zu sein. Sowohl Coles Kritiken als auch zuvor die Ende der 1990er Jahre in den USA einsetzende massive Infragestellung des Fingerabdrucks als gültigem Beweismittel haben teils heftige Reaktionen innerhalb der Kriminalistik ausgelöst und wurden gerade auch innerhalb der informatischen Biometrie zum Anlass genommen, sich einerseits stärker um systematische Belege für die „Individualität von Fingerabdrücken" zu bemühen, andererseits die Bedeutsamkeit der Einzigartigkeit eines Fingerabdrucks in Abhängigkeit vom Anwendungskontext jedoch auch deutlich zu relativieren. Ausführlicher wird dies im Kapitel *Eindeutigkeit, Universalität, Permanenz als Mythos* (4.1) ausgeführt. Außerdem wird im Kapitel *Unterschiede in der Beschreibung der Systemarchitektur* (4.2) erläutert, wie stark die Grundbegriffe und allgemeinen Darstellungen innerhalb des Fachdiskurses noch immer variieren. Akteure der Biometrie-Diskurse und ihre jeweiligen Funktionen und Geschichten werden im Kapitel *Akteure* (4.3) vorgestellt. Schließlich werden am Ende zentrale Eigenschaften des biometrischen Fehlerdiskurses resümiert und bewertet.

4.1 Eindeutigkeit, Universalität, Permanenz als Mythos

Im Jahr 2004 veranstaltete das sowohl privat als auch staatlich finanzierte *Consortium for Mathematics and Its Applications* (COMAP) in den USA den 20. alljährlichen internationalen *Mathematical Contest in Modeling* (MCM) für Oberstufenschülerinnen und Studierende im Bachelor-Studium.[387] Auf diesem Wettbewerb werden in jedem Jahr zwei Problemstellungen formuliert, die offene Fragen in der alltäglichen Lebenswelt darstellen, für die eine sinnvolle mathematische Modellierung gefunden werden soll. Hunderte Teams haben ein Wochenende für gemeinsames Forschen und Modellieren und müssen zum Schluss eine optimale Lösung in Form eines wissenschaftlichen Papers einreichen. Eines der Probleme in jenem Jahr lautete:

> „Are Fingerprints Unique? It is a commonplace belief that the thumbprint of every human who has ever lived is different. Develop and analyze a model that will allow you to assess the probability that this is true. Compare the odds (that you found in this problem) of misidentification by fingerprint evidence against the odds of misidentification by DNA evidence."[388]

[386] Vgl. Krasmann und Kühne 2014, S. 1. Sie beziehen sich hier auf Barthes 1964.

[387] http://www.comap.com/undergraduate/contests, letzter Abruf: 3.8.2017. Das COMAP wird unter anderen finanziert von der *National Science Foundation* (NSF), der *Alfred P. Sloan Foundation*, der *Exxon Education Foundation*, der NSA, dem *United States Department of Education*, *IBM Corporation*, *Texas Instruments* und *Hewlett Packard*.

[388] Garfunkel 2004, S. 190.

Von 203 Einreichungen veröffentlichte die Jury vier, drei davon als herausragend bewertet. Eine trägt den schönen Titel »The Myth of 'The Myth of Fingerprints'«, der den Angriff auf die Wissenschaftlichkeit der Fingerabdruckidentifizierung als den eigentlichen Mythos zurückweist. Die Autoren, Steven G. Amery, Eric Thomas Harley und Eric J. Malm, entwickeln darin ein mathematisches Modell zur Lösung der Problemstellung gemäß der Mitte der 1980er formulierten Kriterien[389] von Stoney und Thornton. Diese wiederum haben dort kritisch ältere mathematische Modelle zur Berechnung der eindeutig unterscheidenden Merkmale von Fingerbildern analysiert. Amery et al. kommen demnach erneut und besser berechnet zu dem Schluss:

> „We compute probabilities that suggest that fingerprints are reasonably unique among all humans who have lived."[390]

Die Einzigartigkeit von Fingerabdrücken könne im forensischen Bereich mit der von DNA mithalten, wenn nicht sogar etwas besser sein – vorausgesetzt, die Qualität der untersuchten Fingerbilder sei ausreichend.

Die stochastische Herleitung der Eindeutigkeit von Fingerabdrücken hat eine lange Tradition voller Irrtümer und Fehler, von denen einige weiter unten kurz referiert werden. Seitens der daktyloskopischen Experten bewegen diese sich weitestgehend in der Logik einer rein wahrscheinlichkeitstheoretischen Analyse des Eindeutigkeitsproblems der phänomenologischen Merkmale des vom Menschen entzifferbaren Fingerbildes, das sich selbstverständlich mit maschineller Sensorik nochmals massiv verschiebt – man denke nur an die Radio-Frequency-Sensoren, die „unter der Epidermis" messen. Hier wird die Kritik Coles und anderer an den dieser Logik zugrundeliegenden Annahmen, der prinzipiellen Beeinflussung dieses „sauberen" mathematischen Diskurses durch spezifische Settings zur Herstellung von Wissenschaftlichkeit und dessen historischer sowie an polizeiliche und wirtschaftliche Interessen gebundene Determiniertheit allerdings ausgeblendet. Die verschiedenen Facetten und Argumente der Diskussion werden im Folgenden genauer vorgestellt.

4.1.1 Berechnungen zur Einzigartigkeit eines jeden Fingerabdrucks

In verschiedenen historischen wie modernen Veröffentlichungen finden sich häufig Ausführungen zur konkreten Möglichkeit des Irrtums bezüglich der extremen Variabilität von Fingerabdrücken, deren exemplarische Ausführung sich an dieser Stelle schon allein deswegen lohnt, um zu zeigen, wie unterschiedlich die vermeintlich auf der Hand liegenden Wahrscheinlichkeiten hergeleitet werden. Maltoni et al. betrachten unter

[389] Vgl. Stoney und Thornton 1986.

[390] Amery, Harley und Malm 2004, S. 215. Ein anderes Team geht sogar noch etwas weiter in seinem Berechnungsergebnis: „[…] we conclude that DNA testing has a higher rate of misidentification." Miller, Mixton und Pickett 2004, S. 259.

Einbeziehung der schon erwähnten Studie von Thornton und Stoney sechzehn verschiedene probalistische Modelle.[391] Diese unterscheiden sich unter anderem anhand der Wahl der Merkmale, mit denen sich die Variabilität von Fingerabdrücken in einer Zielpopulation ausdrücken lässt – viele zielen vor allem auf die in der kriminalistischen Forensik üblicherweise genutzten Minutien unter Hinzuziehung verschiedener anderer Kriterien ab. In der Regel wird die Wahrscheinlichkeit für eine spezifische „Fingerabdruckkonfiguration“[392] berechnet – beispielsweise das Vorkommen einer bestimmten Anordnung bestimmter Minutien innerhalb einer bestimmten Zahl voneinander unabhängiger Regionen der Fingeroberfläche.

Zum Beispiel ermittelte Francis Galton,[393] dass ein Fingerabdruck sich im Durchschnitt in 24 Quadrate zerlegen lässt, die jeweils sechs Papillarlinien überlagern. Verdeckte ein solches Quadrat an einer beliebigen Stelle die Hautleisten, könne man mit einer Wahrscheinlichkeit von $1/2$ den korrekten Linienverlauf anhand der um das Quadrat angrenzenden Regionen erraten – die bedingte Wahrscheinlichkeit für eine spezifische Fingerabdruckkonfiguration sei dementsprechend $1/2^{24}$. Unter Annahme der Unabhängigkeit der Quadrate, mit Einbeziehung der Wahrscheinlichkeit für einen bestimmten Fingerabdrucktyp (Bogen, Delta, Wirbel – Galton typisierte hier 16 verschiedene Typen mit einer Vorkommenswahrscheinlichkeit von $1/16$) sowie einer Wahrscheinlichkeit von $1/256$, dass die richtige Anzahl an Papillarlinien an jeder der 24 Regionen korrekt ein- und austritt, berechnete er

„$P(FingerprintConfiguration) = 1/16 \times 1/256 \times (1/2)^{24} = 1.45 \times 10^{-11}$.“[394]

Eine Übersicht der von verschiedenen Wissenschaftlern teilweise in Kritik vorheriger Modelle berechneten Wahrscheinlichkeiten haben Maltoni et al. zusammengestellt – siehe Tabelle 4.1.

Die Tabelle soll vor allem illustrieren, wie unterschiedlich sich die Einzigartigkeit eines Fingerabdrucks auf Basis verschiedener mathematischer Modelle beziffern lässt. Bis heute stellt das Problem auch mathematisch ein offenes dar, dessen Modellgrenzen sehr klar abgesteckt sein müssen, um es überprüfbar zu machen. Nichtsdestotrotz lässt sich auf Modellebene konstatieren, dass die Variabilität des Fingerbildes so groß ist, dass die Wahrscheinlichkeit, dass zwei Menschen identische Fingerabdrücke haben, extrem gering ist. Doch das mathematische Modell berücksichtigt hierbei allein die Verteilung der unterscheidenden Bildmerkmale ausgehend von höchstmöglicher Bildqualität und lebenslanger Persistenz derselben. Inwieweit eine Maschine oder ein Mensch diese praktisch erkennt, welche Implikationen und Folgen festgestellte Übereinstimmungen haben, berücksichtigen die angeführten Modelle nicht.

[391] Vgl. Maltoni u. a. 2009, S. 345 ff.

[392] Ebd., S. 346.

[393] Vgl. Galton 1892, S. 109 ff.

[394] Maltoni u. a. 2009, S. 346.

Author	P(Fingerprint Configuration)	Probability values for $n = 36, G = 24, B = 72$ ($n = 12, G = 8, B = 24$)
Galton (1892)	$(1/16) \times (1/256) \times (1/2)^G$	$1.45 \times 10^{-11} (9.54 \times 10^{-7})$
Pearson (1930,1933)	$(1/16) \times (1/256) \times (1/36)^G$	$1.09 \times 10^{-41} (8.65 \times 10^{-17})$
Henry (1900)	$(1/4)^{n+2}$	$1.32 \times 10^{-23} (3.72 \times 10^{-9})$
Balthazard (1911) (cf. Stoney and Thornton, 1986)	$(1/4)^n$	$2.12 \times 10^{-22} (5.96 \times 10^{-8})$
Bose (1917) (cf. Stoney and Thornton, 1986)	$(1/4)^n$	$2.12 \times 10^{-22} (5.96 \times 10^{-8})$
Wentwoth and Wilder (1918)	$(1/50)^n$	$6.87 \times 10^{-62} (4.10 \times 10^{-22})$
Cummins and Midlo (1943)	$(1/31) \times (1/50)^n$	$2.22 \times 10^{-63} (1.32 \times 10^{-22})$
Gupta (1968)	$(1/10) \times (1/10) \times (1/10)^n$	$1.00 \times 10^{-38} (1.00 \times 10^{-14})$
Roxburgh (1933)	$(1/1000) \times (1.5/24.12)^n$	$3.75 \times 10^{-47} (3.35 \times 10^{-18})$
Trauring (1963)	$(0.1944)^n$	$2.47 \times 10^{-26} (2.91 \times 10^{-9})$
Osterburg et al. (1977)	$(0.766)^{B-n} (0.234)^n$	$1.33 \times 10^{-27} (1.10 \times 10^{-9})$
Stoney (1985)	$(n/5) \times 0.6 \times (0.5 \times 10^{-3})^{n-1}$	$1.20 \times 10^{-80} (3.50 \times 10^{-26})$

Tabelle 4.1: Die Tabelle stellt knapp die Berechnungen verschiedener Wahrscheinlichkeiten für das Auftreten einer spezifischen Fingerabdruckkonfiguration auf Basis unterschiedlicher Modelle dar. G=24 entspricht der von Galton festgelegten Anzahl von Bildregionen, B=72 ist die Anzahl von Bildregionen bei Osterburg et al. n=36 ist die durchschnittliche Anzahl von Minutien. Tabelle übernommen von Maltoni u. a. 2009, S. 351, © Springer-Verlag.

Die Eigenschaft eines biometrischen Charakteristikums, möglichst langfristig das eindeutige Wiedererkennen einer Person zu ermöglichen, wird sowohl in Bezug auf das Charakteristikum als auch das signalverarbeitende System bezogen stets kontextgebunden relativiert. Sie wird zu einer Systemanforderung, die gegen die anderen abgewogen wird.

4.1.2 Design-Faktoren oder Eigenschaften biometrischer Charakteristika?

Wie bereits im *Kapitel 3.1 Fehler und Biometriesystem-Design* (S. 83) ausgeführt, werden Eindeutigkeit, Universalität und Permanenz im Systemdesign biometrischer Systeme als kategorial äquivalent mit anderen biometrischen Attributen wie Erkennungsgenauigkeit, Akzeptanz der Merkmalsmessung, Erfassbarkeit des Merkmals und ähnlichem betrachtet. Sie erscheinen lediglich als design-relevante Faktoren. Sie sind mindestens genauso relativ wie alle anderen dieser Faktoren. Dementsprechend weisen Bolle et al. folgende Aussage auch als falsch zurück:

> „Biometric X is the 'best' for all applications."[395]

Ihr Argument lautet:

> „There is no single 'best' biometric. Each application and scenario will call for a particular combination of many factors, including price, accuracy, usability, and user acceptance."[396]

Gleichzeitig basiert die Definition der Biometrie – auch in diesem Buch – vor allem auf der einer biometrischen Charakteristik[397] zugeschriebenen Eigenschaft, Individuen voneinander zu unterscheiden:

> „Biometric identification, or *biometrics*, refers to identifying an individual based on his or her distinguishing characteristics."[398]

Ohne die den biometrischen Charakteristika unterstellte Eindeutigkeit wäre Biometrie nicht zu denken, aber man sollte dies wie auch ihre Universalität in der Praxis als flexibel sehen. Die folgende Vereinfachung wird in diesem Sinne ebenfalls als Mythos zurückweisen:

> „Biometric X is unique for each individual."[399]

Es sei zwar ganz klar so, dass die durch genetische Prädisposition und zufällige morphologische Entwicklungsprozesse entstandenen Merkmale lebender Organismen einzigartig seien, aber nur, wenn sie in ausreichender Detailliertheit untersucht würden. Hier gebe es aber klare praktische Grenzen hinsichtlich der Bildauflösung, der Aufnahmebedingungen, des Speicherplatzes, der Vergleichbarkeit erfasster Daten sowie inhärenter persönlicher Schwankungen im Fingerbild über einen längeren Zeitraum.[400]
Im Rahmen grundsätzlicher Design-Entscheidungen gilt es anwendungsbezogen abzuwägen.[401] Yingzi Du wertet beispielsweise physiologische Charakteristika (Gesicht, Finger, Iris, Hand) als relativ stabil über einen längeren Zeitraum, ihre Signalerfassung als einfach und die mit ihnen mögliche Erkennungsgenauigkeit als gut, so dass sie für Identifikation und Verifikation in einer breiten Palette von Anwendungen eingesetzt werden können.[402] Als nicht allzu stabil, nur „somewhat accurate", aber

---

[395] Bolle u. a. 2004, S. 150.

[396] Ebd.

[397] Der Begriff *Biometric* als Substantiv hierfür wird im »Vocabulary« von ISO/IEC inzwischen als überholt zurückgewiesen, vgl. ISO/IEC 2382-37:2017, S. 2.

[398] Bolle u. a. 2004, S. 3.

[399] Ebd., S. 150.

[400] Vgl. ebd.

[401] Siehe auch Tabelle 3.2, S. 86.

[402] Vgl. Du 2013, S. 3.

ebenfalls einfach zu erfassen, betrachtet sie verhaltensgebundene Merkmale (Handschrift, Gang, EEG, Atemmuster, Herzschlag).[403] Die psychologischen Charakteristika (Hirnfunktionen oder kognitionsbasierte Systeme) schließlich, die noch in einem frühen Entwicklungsstadium seien, würden zur Zeit noch eine schlechte Erkennungsgenauigkeit haben, über längere Zeit sehr instabil – also kaum tauglich zur Identifikation oder Verifikation – sowie sehr schwer zu erfassen sein.[404] Im Grunde entsprächen sie zwar definitorisch nicht mehr biometrischen Charakteristika, aber dass sie überhaupt sensorisch erfassbar, digitalisierbar und eventuell im biometrischen Kontext einsetzbar scheinen, genüge. So könnten sie unterstützend in Hochsicherheitsbereichen genutzt werden, um festzustellen, ob die betroffene Person lebt und sich willentlich dem Authentifizierungsprozess unterzieht.[405]

Die Untergliederungen biometrischer Charakteristika in biologische/physiologische, verhaltensbedingte oder psychologische sind ebenfalls umstritten. Im »Vocabulary« der ISO/IEC wird beispielsweise konstatiert, dass biologische und verhaltensbezogene Charakteristika nicht immer klar voneinander zu unterscheiden seien, da bspw. das Bild eines Fingerabdrucks sowohl durch die Struktur der Papillarlinien auf dem Finger als auch durch die Art der Präsentation des Fingers am Sensor bestimmt sei.[406] Von biometrischer Relevanz würde dieses Verhalten allerdings wohl nur sein, wenn es bei jedem Menschen einzigartig wäre.

Alles in allem ist sowohl die Fixierung auf ein spezifisches Charakteristikum und eine klare Eingrenzung dessen einzigartiger Anteile eine höchst fragile Angelegenheit. Insgesamt legen Bolle et al. daher einen Begriff der Indiviualität eines biometrischen Merkmals vor, der auf dessen Abbildbarkeit mittels maschineller Repräsentation abhebt, also eine Frage der algorithmischen Konstruktion ist:

> „Individuality [of a biometric] has to do with how different one machine representation can be from another, and how many different representations there are.“[407]

Auch was die Permanenz einer biometrischen Charakteristik angeht, wird diese in den wissenschaftlichen Veröffentlichungen selbst für die Fingerabdruckbiometrie deutlich relativiert. Die Frage nach der lebenslangen Unveränderlichkeit des Fingerabdrucks stellt sich ebenfalls auf zweierlei Weise: zum einen in Bezug auf die körperliche Veränderung der Charakteristik, zum anderen in Bezug auf die Veränderung der Abbildung des Abdrucks, also etwa des digitalen Templates über die Zeit. Der Begriff *Template Ageing* vereint diese Aspekte:

---

[403] Ebd.

[404] Vgl. ebd., S. 2 f.

[405] Vgl. ebd., S. 3.

[406] Vgl. ISO/IEC 2382-37:2017, S. 2, Anmerkung 5, Begriff „biometrics“.

[407] Bolle u. a. 2004, S. 151.

> „Template ageing refers to the increase in error rates caused by time related changes in the biometric pattern, its presentation, and the sensor.“[408]

Kevin Bowyer und seine Kollegen konnten 2012 die von Daugman in Bezug auf Iriserkennung postulierte These, „that the iris texture is stable over a person's life“ durch eine umfassende Studie widerlegen. Sie konstatierten in diesem Zusammenhang, dass eine derartige Untersuchung der Template-Alterung für Fingerabdrücke nie vorgenommen wurde.[409] Bekannt ist allerdings, dass sich sowohl die Abdrücke von Kindern in Bezug auf die Abstände und gute Ausprägung der Hautleisten noch verändern, wenngleich der Linienverlauf gleich bleibt, als auch, dass die langfristige Hautalterung sowie die individuelle Lebensführung (Narben durch Unfälle, starke Hautabnutzung bei bestimmten Berufen) ihre Spuren hinterlassen. Beide Aspekte stellen spezielle Anforderungen an die Abnahme eines Fingerbildes.[410]

Schließlich sind Fingerabdrücke nicht bei jeder universell. Gary Roethenbaugh formuliert es als eine zu lernende Wahrheit:

> „Physical characteristics vary and some individuals will not be able to use a biometric system.
> […] the important lesson to be learnt is that no single biometric system can capture and match biometric data for the global population in all circumstances. Human beings are as diverse and unpredictable as environments. […] A small minority of individuals have damaged fingers […] It is simply that the minority cannot use the system automatically and must be dealt with in an appropriate manner.“[411]

Zur Größe der „kleinen Minderheit“ finden sich in der Literatur unterschiedliche Aussagen. Für etwa vier Prozent der Bevölkerung sei nach nicht näher genannten Studien empirisch belegt, dass sie Fingerabdrücke sehr schlechter Qualität für existierende Sensoren lieferten, schreiben etwa Jain und Ross.[412] Maltoni et al. wiederum sprechen von zehn Prozent („according to our experience“).[413] Hicklin, Ulery und Watson erläutern, dass häufig die Zahl von zwei Prozent aus einem Bericht des NIST zitiert werde. Sie korrigieren diese Zahl aufgrund von Daten des Grenzkontrollidentifikationssystems US-

[408] Mansfield und Wayman 2002, S. 16.

[409] Fenker und Bowyer 2012, S. 1.

[410] Vgl. Rebera und Guihen 2017.

[411] Roethenbaugh 1998, Section 5.

[412] Vgl. Jain und Ross 2004. Ebenfalls unbelegt findet sich diese Zahl in einem Bericht der Europäischen Kommission zu großflächigem Biometrie-Einsatz (vgl. Goldstein u. a. 2008, S. 63). Dort findet sich allerdings auch die vage Behauptung: „It is also said that Asian people have difficult fingerprints to read.“ (ebd.). Dagegen spricht allerdings die Nutzung des Fingerabdrucks für Grenzkontrollen oder Bezahl-Applikationen beispielsweise in Japan. Außerdem waren keine wissenschaftlich publizierten Studien hierzu zu finden.

[413] Maltoni u. a. 2009, S. 131.

VISIT deutlich nach unten: Nur zwischen 0,2 % und 0,5 % der kontrollierten Personen hätten aufgrund von Hautkrankheiten oder einer Disposition für nicht-vorhandene Abdrücke häufiger einen *False Match* erzielt.[414] Sie schränken allerdings auch ein, dass dieser Prozentsatz für viel mit den Händen arbeitende oder ältere Menschen höher sein dürfte. Die meisten Probleme entstünden aber nicht wegen intrinsischer Defizite, sondern aufgrund ungeeigneter, weniger akkurater Software und schlechter Qualitätskontrollprozeduren für die aufgenommenen Bilder der Merkmale. In sehr seltenen Fällen seien erblich bedingt bei einigen Menschen gar keine Papillarlinien an den Händen vorhanden.[415] Weitere Möglichkeiten sind natürlich auch fehlende Finger.

Ein üblicher Vorschlag ist in diesem Zusammenhang der Verweis auf multimodale Biometrie, bei der man auch auf andere messbare biometrische Merkmale ausweichen kann. Diese kann allerdings wiederum negative Auswirkungen auf Kosten, Bearbeitungsgeschwindigkeit und auch Erkennungsgenauigkeit haben. Darauf weisen Bolle et al. hin, wenn sie die Annahme, dass Multi-Biometrie leistungsfähiger sei als nur auf einer Charakteristik beruhende, als Mythos benennen.[416]

Gerade in Bezug auf Fingerbilder schlechter Qualität gibt es als weiteren Lösungsansatz kontinuierliche Verbesserungen der Sensorik sowie der Merkmalsextraktionsalgorithmen.[417]

Es lässt sich allgemein zusammenfassen, dass der innerfachliche Diskurs zu dem Ergebnis kommt, dass die biometrischen Charakteristiken gemeinhin zugeschriebenen Eigenschaften der Einzigartigkeit, Dauerhaftigkeit und universellen Messbarkeit gerade im Licht der Automatisierung zu flexiblen Konstruktionen werden müssen. Nur durch geeignete Modellierung können sie annähernd abgebildet werden und stehen dann zudem in der Gefahr, etwas abzubilden, das vielleicht gar nicht in dieser Form vorhanden ist. Das Ziel der mathematischen Modellierungen, aus der Diversität des Fingerbildes die gewünschten eindeutigen und ewig universalen Identifikationsmerkmale zu berechnen, ist zudem zwar ein ausgeklügeltes spannendes Mustererkennungsproblem, aber gerade hinsichtlich des dahinter steckenden essentialistischen Personenkonzepts eben keine angewandte Mathematik, sondern eher zutiefst „anwendungsvergessen“.[418]

---

[414] Vgl. Hicklin, Ulery und C. Watson 2005.

[415] Burger et al. geben ihrer Studie, in der sie von lediglich vier weltweit klinisch dokumentierten Familien berichten, in denen in mehreren Generation die Adermatoglyphia genannte Abwesenheit von Hautleisten an den Händen vorkommt, den zynischen Titel »The immigration delay disease«, da sie mit dem Fall einer Schweizerin konfrontiert wurden, die deswegen nicht in den USA einreisen konnte, vgl. Burger u. a. 2011.

[416] Vgl. Bolle u. a. 2004, S. 152.

[417] Siehe bspw. Ryu, Kong und Kim 2011.

[418] Siehe hierzu auch die Ausführungen am Ende, im *Kapitel 4.4 Fazit* (S. 165).

4.1.3 Infragestellung des Fingerabdrucks als Beweismittel

„In 1893, the Home Ministry Office, UK, accepted that no two individuals have the same fingerprints.“[419] Dass die Akzeptanz dieser Tatsache nie wirklich umfassend systematisch begründet und empirisch überprüft wurde und die daktyloskopische Expertise eine Institutionalisierung erfuhr, die sie scheinbar unentbehrlich machte, leitet Cole, der im Rahmen diesbezüglicher Erörterungen auch meistens angeführt wird, ausführlich historisch her. Maltoni et al. übernehmen Coles Sichtweise:

> „The scientific basis of fingerprint individuality continues to be questioned in the courts of laws in the United States to this day […]. Thus the uniqueness of fingerprints is neither a bygone conclusion nor has it been extensively studied in a systematic fashion.“[420]

Im rechtswissenschaftlichen Bereich begann der Angriff auf den Fingerabdruck als Beweismittel mit dem Gerichtsprozess *United States of America versus Byron Mitchell*,[421] in dem auf die im Verfahren *Daubert versus Merrell Dow Pharmaceuticals*[422] 1993 festgelegten Kriterien für die Wissenschaftlichkeit einer Beweismethode zurückgegriffen wurde. Im Rahmen einer sogenannten „Daubert-Anhörung“ wird geprüft, ob eine Sachverständigenaussage, wie sie beispielsweise eine Kriminaltechnikerin oder eine Daktyloskopin abgibt, auf einer getesteten, durch Peer-Review überprüften Methodologie beruht, deren Fehlerraten bekannt sind. Der Fingerabdruck als Beweismittel hielt den Prüfungen im Rahmen der bisherigen gerichtlichen Auseinandersetzungen stand.[423]

Eine erfolgreichere Strategie als die Daubert-Anhörungen zur Widerlegung der Tauglichkeit des Fingerabdrucks als Beweismittel war die Heranziehung von DNA-Tests zu Unrecht verurteilter Menschen. Öffentlichkeitswirksam hat vor allem das 1992 gegründete *Innocence Project* in den USA bis heute 330 Menschen durch DNA-Tests entlasten und ihre Befreiung bewirken können.[424] Die Vertreter der Organisation, in der sich verschiedene „nonprofit legal clinics and criminal justice resource centers“ ver-

---

[419] Maltoni u. a. 2009, S. 1.

[420] Ebd., S. 36. Sie widmen sich daher ausführlich im bereits referenzierten Kapitel »Fingerprint Individuality« den bisherigen Untersuchungen zu dieser Frage (vgl. ebd., S. 341 ff.). Hierbei übernehmen sie zu großen Teilen einen zuvor veröffentlichten Artikel (siehe Pankanti, Prabhakar und Jain 2002).

[421] US v. Byron Mitchell, Criminal Action No. 96–407. July 7–13, 1999. US District Court for the Eastern District of Pennsylvania.

[422] Daubert v. Merrell Dow Pharmaceuticals, Inc. 113 S. Ct. 2786. 1993.

[423] Vgl. Romandetti 2004. Siehe außerdem zur fortgeführten Auseinandersetzung Cole 2005a sowie Cole 2005b.

[424] http://innocencenetwork.org, letzter Abruf: 28.7.2017. Siehe auch Simon, P. Neufeld und B. Scheck 2003.

einen,[425] fungieren als *Amicus Curie* (Freund des Gerichts) und steuern ausführliche Gutachten in wieder aufgenommenen Verfahren bei. Sie verweisen beispielsweise im Gutachten für den Fall *Bobby Lee Holmes versus The State of South Carolina*[426] auf drei weitere „prominente" Fingerabdruckirrtümer der Forensik – einer davon die Verhaftung des Anwalts Brandon Mayfield im Zusammenhang mit dem Bombenanschlag gegen einen Pendlerzug im März 2004 in Madrid, dem 191 Menschen zum Opfer fielen.[427] Obwohl es nur in wenigen Fällen des *Innocence Project* real um Fehlinterpretationen oder die gar nicht eindeutige Zuordnung von Fingerabdrücken ging, ist es doch bemerkenswert, dass der DNA-Test gewissermaßen den Fingerabdruck als biometrisches Merkmal sticht, seine Evidenzkraft wesentlich mächtiger ist. Er scheint nicht nur Fehler in der forensischen Beweisführung, sondern vor allem auch Fehlidentifikationen von Augenzeugen, schlechte Verteidigung des Angeklagten, falsche Geständnisse oder ähnliches wieder wettmachen zu können. Ein biometrisches Charakteristikum wird hier zu einem Hebel, ein insgesamt nachweislich schlecht durchgeführtes und von Vorurteilen durchsetztes, komplexes Verfahren wieder aufzurollen. Manchmal geht es auch einfach nur darum, erneut einen DNA-Test zu machen, weil die ersten so schlecht durchgeführt wurden.[428] Eine Einforderung der Einhaltung hoher Standards bei der Heranziehung von forensischen Beweisen ist letztlich Teil des „post-conviction DNA litigation model",[429] das die Organisation verfolgt. So gibt es einige Fälle, in denen Fingerabdrücke die Unschuld der Angeklagten gestützt hätten, sie wurden aber im Fortgang der Beweisführung nicht dementsprechend gewichtet.[430]

Zusammenfassend lässt sich sagen, dass die Kritik am Fingerabdruck als Beweismittel im Rahmen der Daubert-Anhörungen vor allem auf Verfahrensfehler abzielt. Das heißt etwa, dass sehr hohe Anforderungen an eine genaue Abnahme der Abdrücke gestellt werden, dass eine stärkere Formalisierung nötig ist. Die Nutzung der DNA-Biometrie zum Beweis der Unzulänglichkeit des Fingerabdrucks zeigt, dass die prinzipielle Idee eines objektiven, eindeutigen, biologisch unveränderlichen Merkmals einer Person, das sie immer zweifelsfrei identifiziert, oder die Idee einer Strafnotwendigkeit hier nicht in Frage gestellt wird. Cole kündigt deswegen nicht zu Unrecht in seinem Buch von 2001 an, dass die DNA der moderne Fingerabdruck werden könnte – wie uns allerdings die oben zitierten Papers des *Mathematical Contest in Modeling* zeigen, ist selbst dieser Wettlauf nicht entschieden.

---

[425] Park 2017, S. 1.

[426] Bobby Lee Holmes v. The State of South Carolina. No. 04–1327.2005. Supreme Court of South Carolina.

[427] Vgl. B. C. Scheck, P. J. Neufeld und Metlin 2005.

[428] http://www.innocenceproject.org/cases-false-imprisonment/steven-barnes, letzter Abruf: 28.7.2017.

[429] Park 2017, S. 1.

[430] So in den Fällen von Kenny Waters, James Ochoa und Steven Barnes (siehe in der Datenbank http://www.innocenceproject.org/cases, letzter Abruf: 28.7.2017).

4.2 Unterschiede in der Beschreibung der Systemarchitektur

Die schematischen Visualisierungen und die Beschreibung der generischen Systemarchitektur eines biometrischen Systems legen nahe, dass es eine modulare Grundstruktur besitzt, bei dem sich die einzelnen Systemkomponenten praktisch auswechseln lassen. Eine Fehleinschätzung, die Bolle et al. beispielsweise in Bezug auf die Trennung von Merkmalsextraktions- und Vergleichsmodul als Mythos bezeichnen. Eine Aussage wie die folgende gehört dazu:

> „Our feature extractor can be used with any match engine."[431]

Feature-Extraktionsalgorithmen produzieren je nach Implementierung geringfügig voneinander abweichende Features. Die Normierung des Template-Formats selbst hat erst einmal wenig damit zu tun, auf welche Weise die in den Templates gespeicherten Merkmalsvektoren im Bild gefunden wurden. Daher ist es sinnvoll, ein Vergleichsmodul (hier die „match engine") zusammen mit dem Merkmalsextraktor zu entwickeln „with each adapted to the biases of the other".[432] Die Vergleichswahrscheinlichkeiten ändern sich nämlich je nach entdeckten Features.

Die Normierung der Komponentenschnittstellen und -datenformate ermöglicht zwar prinzipiell eine höhere Modularität – ein einfaches und beliebiges Austauschen ohne Performanzverlust ist allerdings dennoch unrealistisch, zumal die Konformanz mit den jungen internationalen Normen ebenfalls nicht generell gegeben ist.

Zudem ist die Vereinheitlichung der Grundbegriffe im wissenschaftlichen Diskurs ebenfalls noch sehr frisch. Ein folgender Exkurs in die in der Literatur sehr unterschiedlichen Beschreibungen einer allgemeinen Biometrie-Systemarchitektur soll die Dynamik der grundlegenden Begriffe stärker verdeutlichen.

Das 2007 im »Biometrics Tutorial« veröffentlichte generische Modell ähnelt textlich wie graphisch stark den Darstellungen in verschiedenen Artikeln von James L. Wayman in den Jahren zuvor. Abbildung 4.1 zeigt eine der von Wayman geprägten Varianten[433] im Vergleich mit der aktuellen des SC37.[434] Diese wiederum schließen an die Arbeiten des vom *Biometric Consortium* ins Leben gerufenen *National Biometric Test Centers* an der *San Jose State University* (1997–2000) an, das die Herausbildung eines verallgemeinerten Systemmodells und eines vereinheitlichten Vokabulars maßgeblich beeinflusst hat.[435] Auch Roethenbaugh hat Ende der 1990er Jahre in Zusammenarbeit

[431] Bolle u. a. 2004, S. 152.

[432] Ebd.

[433] Andere Varianten sind in Wayman 2000, S. 6 oder Wayman 2005, S. 10 zu finden.

[434] Vgl. ISO/IEC TR 24741:2007, S. 9 ff. Das Modell wird absehbar aktualisiert. Laut ISO/IEC JTC 1/SC 37 N 5831, S. 1 wird der Inhalt des ISO/IEC JTC 1/SC 37 N 3972 übernommen. Dieser ist wesentlich kompakter und übernimmt die aktuelle Terminologie des »Vocabulary«.

[435] Vgl. Wayman 2000, S. iii.

mit Tony Mansfield (*Association for Biometrics*, AfB) ein »Glossary of Biometric Terms« herausgegeben. Außerdem beziehen sich die Architekturbeschreibungen des »Biometrics Tutorial« und der anderen ISO-Veröffentlichungen ganz wesentlich auf die Standardisierung der Implementierungsarchitektur BioAPI, die Austausch- und Interoperabilitätsdatenformate BIR und BDB[436] und referenzieren auch deren Begrifflichkeiten für Datenformate und die Beschreibung interner Systemschnittstellen.

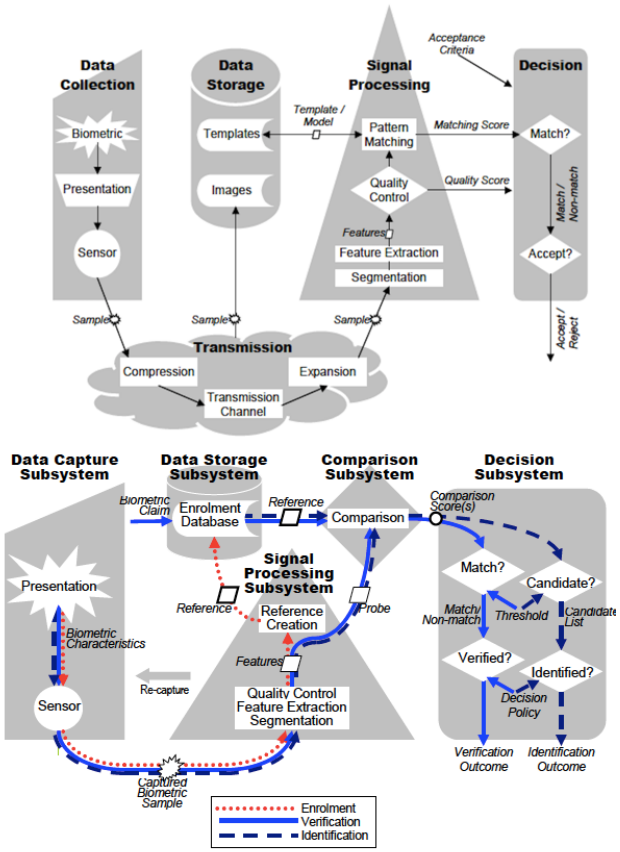


Abbildung 4.1: Das obere Bild zeigt eine Variante der von Wayman/Mansfield Ende der 1990er, Anfang der nuller Jahre entwickelten Schemata aus Mansfield und Wayman 2002, S. 2 im Vergleich mit der sehr ähnlichen aktuellen grafischen Darstellung, die im Einklang mit den vom SC37 entwickelten Begriffen steht, aus ISO/IEC JTC 1/SC 37 N 3972, S. 1 © ISO/IEC.

[436] Vgl. ISO/IEC TR 24741:2007, S. 18 ff. Die zugehörigen, mehrteiligen Standards sind »ISO/IEC 19784 Information Technology – Biometric application programming interface«, »ISO/IEC 19785 Information technology – Common Biometric Exchange Formats Framework», »ISO/IEC 19794 Information technology – Biometric data interchange formats« und der nur ein Dokument umfassende Standard »ISO/IEC 24708 Information technology – Biometrics – BioAPI Interworking Protocol«.

Biometrische Systeme werden zumeist mittels Flussdiagrammen ihrer Prozesskomponenten nach dem Eingabe-Verarbeitung-Ausgabe-Prinzip schematisch visualisiert.
Während Abbildung 4.1 Enrolment, Verifikation und Identifikation nur mit unterschiedlichen Pfeilen darstellt, trennen andere Grafiken wie bspw. die von Jain, Flynn und Ross diese drei Prozesse visuell voneinander (siehe Abbildung 4.2).[437]

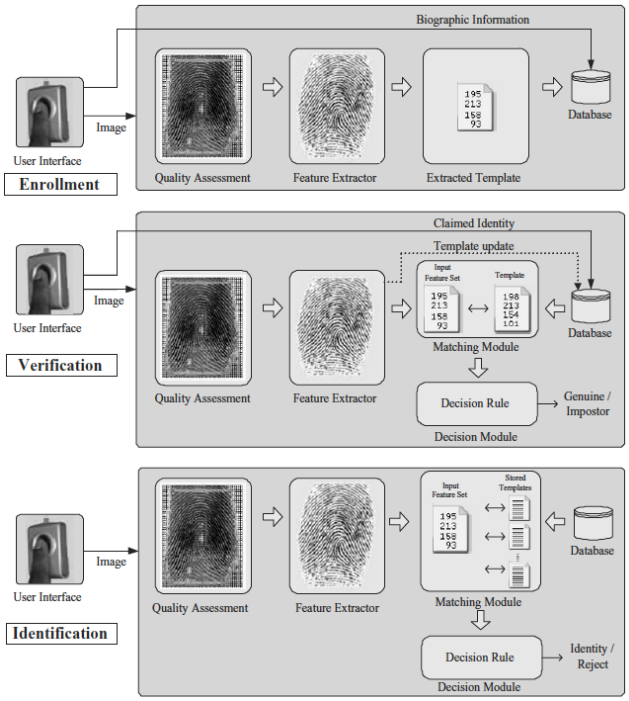


Abbildung 4.2: Blockdiagramm aus Jain, Flynn und Ross 2008a, S. 7, © Springer-Verlag.

Betrachtet man nun die einzelnen Komponenten detaillierter, so lassen sich folgende Unterschiede feststellen:

- Das *Biometric Capture Subsystem* – *die* Mensch-Maschine-Schnittstelle zur Dateneingabe – fasst oft unterschiedliche Teilaspekte zusammen. Als *User Interface* bezeichnen es nur Jain et al. (siehe Abbildung 4.2). In deren Grafik scheint das *User Interface* nur der Aufnahme des Fingerabdrucks zu dienen. In den anderen Grafiken ist dies ähnlich: Nur die Präsentation der Charakteristik ist abgebildet. In den Texten ist dagegen zusätzlich die Rede davon, dass über ein *User Interface* gegebenenfalls auch weitere Daten wie Name oder Identifikationsnummer eingegeben werden können.[438]

[437] Das Schema bei Maltoni et al. ist ebenso aufgebaut, nur etwas weniger bildhaft, siehe Maltoni u. a. 2009, S. 4.

[438] Vgl. Jain, Flynn und Ross 2008a, S. 5.

Die deutlich separierte Platzierung der Nutzerinnenschnittstelle von den in einem Rechteck zusammengefassten restlichen Teilmodulen unterscheidet die grundsätzliche grafische Gruppierung von Jain auch von vielen anderen Darstellungen, in denen die Erfassung gleichwertig zum System zu gehören scheint. Demgegenüber kommt ihr allerdings in den meisten textlichen Erläuterungen sehr wohl eine besondere Rolle zu, da alle Messungen und Entscheidungen des Systems von dem Sensor-Output abhängen. So werden etwa die biometrische Charakteristik selbst, die Art und Weise, wie und in welchen Umgebungsbedingungen sie präsentiert wird – und damit das Verhalten der betroffenen Person –, sowie die technischen Eigenschaften des Sensors als zu berücksichtigende Teile des Erfassungssubsystems in den verschiedenen Texten betont und im Bild stark abstrahiert mit einem vielzackigen Polygon dargestellt, das sonst kein übliches Darstellungselement in Prozessablaufplänen ist.

- Ebenfalls unterschiedlich wird dargestellt, wann und in welcher Abfolge *signalverarbeitende Prozesse* stattfinden und was sie umfassen. Faktisch beginnt die Signalverarbeitung schon mit der Erfassung von Licht, Kapazität, Schwingungen oder ähnlichen Signalen am Sensor, dennoch ist dies oft nicht so beschrieben. In den Beispielen in Abbildung 4.1 werden Datenerfassung und Signalverarbeitung voneinander separiert betrachtet. Die Erwähnung von Teilprozessen der Signalverarbeitung wie *Segmentation*, *Quality Control* oder *Feature Extraction* erfolgt in unterschiedlichen Reihenfolgen oder Zuordnungen. Bei Jain et al. nimmt die *Qualitätskontrolle* zum Beispiel eine herausragende Stellung noch vor der Merkmalsextraktion ein. Sie erwähnen im Text, das typischerweise das Signal nach der Erfassung verbessert würde (*Signal Enhancement*), aber wenn die Qualität der Daten dennoch nicht ausreiche, die Nutzerin erneut die biometrischen Daten präsentieren müsse.[439] Dies wird im Schema der SC37 durch den *Recapture*-Pfeil angedeutet.

  Der Kontrollfluss, der anzeigt, dass auch die Qualitätskontrolle den Entscheidungsprozess beeinflussen kann, etwa durch Übernahme höherer Anforderungen bei einem Sample schlechter Qualität, wie man es im oberen Schema in Abbildung 4.1 sieht, ist in den anderen Grafiken nicht zu sehen, aber wird teilweise im Text erwähnt.[440]

- Die *Feature Extraction* fehlt in den gezeigten Beispielen nirgends und ist insbesondere bei Jain et al. und Maltoni et al. ein zentrales alleinstehendes Modul. Sie ist häufig proprietär implementiert, „obwohl die standardisierten BDB-Formate, die Merkmale aufnehmen, ausreichend Anleitung dafür bieten, wie Merkmals-

[439] Vgl. ebd.

[440] Vgl. ISO/IEC TR 24741:2007, S. 11.

extraktion für diese Formate abläuft."[441] Die Ignoranz dieser Möglichkeit führt dann häufig auch zu dem eingangs des Kapitels erwähnten Problem, das gerade nicht-standardkonforme Module integriert entwickelt werden müssen.

- Der Begriff des *Pattern Matching*, der bei Wayman et al. als Teilprozess der Signalverarbeitung genannt wird,[442] dort auch so in der Grafik auftaucht, findet sich auch noch im »Biometrics Tutorial«, hier im Text synonym für das *Matching Subsystem* gebraucht.[443] In den anderen Veröffentlichungen ist er eher für sehr konkrete Vergleichsalgorithmen gebräuchlich und ist im Allgemeinen ungünstig gewählt, da er exakte Übereinstimmungen zwischen Mustern suggeriert und nicht Ähnlichkeiten, wie in der Biometrie der Fall.

  Ferner ist dieser *Vergleichsprozess* als *Comparison* oder *Matching Module* als zentrale Komponente in allen anderen Beschreibungen extra dargestellt. *Matching* ist ein Begriff, den das »Vocabulary« der ISO/IEC schließlich in seiner Verwendung stark eingeschränkt hat, da er zu vieldeutig verwendet worden sei[444] – *Comparison* sei der geeignetere Begriff.

- Maltoni et al. wiederum verzichten auf die abgetrennte grafische Auszeichnung eines *Entscheidungsmoduls* (*Decision Subsystem*), sondern stellen dies als Teil des Vergleichs dar, dessen Resultat die Ausgabe eines *Match/Non-Match*, eines *Subject Identifier* oder der Meldung *Not Identified* ist. Im Text allerdings geben sie an, dass die Ausgabe des *Matching Module* typischerweise ein *Matching Score* sei.[445]

- Recht unterschiedlich sind die die *Entscheidung* beeinflussenden Faktoren bezeichnet. *Acceptance Criteria* (in anderen Darstellungen auch nur *Ancillary Information*) fließen bei Wayman/Mansfield (siehe Abbildung 4.1) erstaunlicherweise mit einem im Leeren beginnenden Pfeil zusätzlich mit dem *Matching Score* in die Entscheidung ein. Diese Zusatzinformationen stellen die im Text als *Decision Policy* oder *System Policy* angeführten Management-Entscheidungen dar, die spezifisch für die operationalen und Sicherheitsanforderungen eines biometrischen Systems sind. Diese sind in der unteren Grafik denn auch im *Decision Subsystem* als *Decision Policy* integriert. Auch der administrativ veränderbare *Schwellwert*, ab dem eine Ähnlichkeit in Bezug auf den aus dem Vergleichssystem einfließenden *Similarity Score* einen *Match* oder eine Kandidatenauswahl bedeutet, ist hier gezeigt. Bei Jain et al. tauchen diese Parameter wiederum nur

[441] ISO/IEC TR 24741:2007, S. 12, von Verfasserin übersetzt.

[442] Vgl. Wayman, Jain u. a. 2005, S. 10.

[443] Vgl. ISO/IEC TR 24741:2007, S. 13.

[444] Vgl. Wayman, McIver u. a. 2014, S. 7.

[445] Vgl. Maltoni u. a. 2009, S. 14.

kurz als *Decision Rule* auf. Diese Regeln sind entscheidend für das Verhältnis der unvermeidlichen falschen Entscheidungen des Moduls (siehe auch Unterkapitel 3.2.2), die durch entsprechende, in keiner der Grafiken modellierte Ausnahmebehandlungen gemildert werden.

Gerade der im Außen beginnende Pfeil der *Acceptance Criteria* der inzwischen durch die Autoren selbst überholten Grafik kann als Anknüpfung an viele in diesem Modell nicht darstellbare Komponenten gelesen werden. In seiner Beiläufigkeit zeigt er zudem, dass in der gängigen technischen Reduktion diese Faktoren als unwesentlich für die Modellierung der Funktionalität des Biometrie-Systems betrachtet werden.

In der Grafik von Wayman/Mansfield gibt es gar keine sichtbare Trennung von Identifikation und Verifikation wie in allen anderen Grafiken. Im Text hierzu findet sich die Argumentation, dass diese beiden Sichtweisen im Grunde nicht wirklich informativ und eher historischer Natur seien.[446]

Ferner fehlt – außer bei Wayman/Mansfield – der beispielsweise im »Biometrics Tutorial« zwar im Text erwähnte in beide Richtungen laufende Steuerungsfluss zwischen Entscheidungssubsystem und Datenbanksystem wie etwa das Auslösen einer Datenbanksuche oder das Abrufen zusätzlicher Templates.[447]

- Allein in der Grafik von Wayman/Mansfield ist ein *Transmission-Subsystem* überhaupt jenseits von in allen Schemata verwendeten Datenübertragungs- und Kontrollflusspfeilen als eigenes Modul abgebildet. Allerdings wird es bei allen Autoren spätestens bei der Erörterung der Datensicherheit doch einbezogen, da es einen zentralen Angriffspunkt darstellt.[448]

  Bei Wayman/Mansfield werden die Subprozesse dieses Teilsystems mit dem klassischen Shannon-Weaver-Kommunikationsmodell zur Übertragung eines kodierten Signals über einen Kanal abgebildet. Auch im »Biometrics Tutorial« wird auf dieses Teilsystem zumindest im Text hingewiesen sowie spezielle technische Problemstellungen diesbezüglich kurz erläutert.[449]

  Die Anordnung des Transmissionsteilsystems zwischen Datenerfassung und Signalverarbeitung wie bei Wayman/Mansfield ist jedoch willkürlich, da dieses Teilsystem letztlich alle Schnittstellen der Subkomponenten verbindet.

- Auch die Ausdifferenzierung des *Speichermoduls* (*Data Storage*) in Wayman/Mansfield fällt aus den anderen grafischen Komponentenmodellierungen her-

[446] Vgl. Wayman, Jain u. a. 2005, S. 6 f.

[447] Vgl. ISO/IEC TR 24741:2007, S. 13.

[448] So zum Beispiel bei Maltoni u. a. 2009, S. 383 ff.

[449] Vgl. ISO/IEC TR 24741:2007, S. 10.

aus. Im *Data Storage*-Teilsystem werden *Templates* von *Images*, die gerade aufgenommene Rohdaten repräsentieren, sichtbar symbolisch getrennt. *Templates* sind bereits biometrisch prozessierte Daten, das heißt, die Merkmale sind bereits aus den Samples extrahiert. Im »Biometrics Tutorial« wird diese Möglichkeit im Text erwähnt.

Neben den im Detail recht unterschiedlichen Begriffsbezeichnungen wird in allen Visualisierungen deutlich, dass einige die Funktionalität ganz entscheidend beeinflussende Aspekte wie die eben genannten System- und Entscheidungsregeln, die operativen Bedingungen (Art der Präsentation, Umgebungsverhältnisse, Personal) oder das Datenmanagement nicht im Zentrum der visualisierten generischen Modellierung eines Biometrie-Systems stehen. Zwar deuten die Pfeile zumindest in Teilen den Kontrollfluss zwischen einzelnen Modulen und während bestimmter funktionaler Modi wie Enrolment, Verifikation und Identifikation an, und verbal werden auch Kontrollbedingungen wie Schwellwert oder Entscheidungskriterien bezeichnet. Der Fokus der basalen funktionalen Erläuterung aber liegt auf der Transformation sensorisch als Samples erfasster Daten zu Features/Templates/Modellen/Referenzen, die entweder gespeichert oder mit anderen bereits gespeicherten Daten verglichen werden. Der Vergleich mündet über die einem Schwellwert genügende Ähnlichkeit oder Unähnlichkeit zweier Features/Templates/Modelle/Referenzen in einer Verifikations- oder Identifikationsentscheidung.

Keine der Darstellungen gibt trotz aller kleineren auffälligen Unterschiede die grundsätzliche Anmutung eines Flussdiagramms auf. Die Modellierung in Abbildung 4.1 nutzt für die Subsysteme jeweils die üblichen Symbole: Für *Data Capture* wurde das Trapez als Zeichen für manuellen Input, für *Signal Processing* das Dreieck als Zeichen für eine Extraktions-, Zerlegeoperation, für *Data Storage* der Zylinder und für *Comparison* das Rhombus gewählt. Das Rechteck mit abgerundeten Ecken für *Decision* könnte als Terminator-Prozess interpretiert werden, ist aber eher unkonventionell in der längs aufgezogenen Form. Lediglich das Symbol für die *Presentation* fällt, wie schon erwähnt, als ungewöhnlich auf. In Abbildung 4.2 wird nur auf Prozess-Rechtecke, Speicherzylinder und Flusspfeile zurückgegriffen. Sensor und Präsentation der biometrischen Charakteristik werden allerdings als eine den Vorgang einer Zeigefingerabdruckabnahme an einem optischen Sensor wiedergebende Fotografie gezeigt. *Quality Assessment* und *Feature Extractor* werden mit grafischen Repräsentationen des Fingerbildes in dem entsprechenden Stadium veranschaulicht. Templates werden dort mit dem Icon für eine Textdatei, die eine Liste von Dezimalzahlen zeigt, abgebildet.

Den Grafiken ist prinzipiell aber gemeinsam, dass Pfeile die sequentielle Abfolge von Prozessen und Subprozessen vorgeben, die in voneinander getrennten geometrischen Grundfiguren stattfinden oder mehrere bündeln. Allerdings münden die Flüsse nach dem Entscheidungsprozess nicht – wie bei solchen Diagrammen üblich – in Terminatorrechtecken oder -ellipsen. In Abbildung 4.2 verbleiben sie innerhalb der das ganze

System umschließenden Rechtecke, in den anderen Grafiken führen die Pfeile sogar aus dem Diagramm hinaus. Der Schlusszustand an den jeweiligen Pfeilenden wird überall jeweils lediglich verbal und sehr unterschiedlich als *Verification Outcome* und *Identification Outcome* oder als Entscheidung zwischen zwei Zuständen wie *Genuine* oder *Impostor*, *Identity* oder *Reject* oder als *Accept* oder *Reject* bezeichnet. Eine Entscheidung, die dann dem nicht dargestellten Systemäußeren so zur Verfügung steht. Das »Vocabulary« der ISO/IEC lässt sogar die Möglichkeit zu, dass es ein Weder-noch, ein *Undetermined*, als mögliche *Comparison Decision* gibt, allerdings nur in einer Anmerkung zu diesem Begriff.[450]

Zuletzt bleibt noch die Frage, in welcher Rolle der Mensch innerhalb dieser Visualisierungen auftaucht. Die Interaktion zwischen System und Mensch wird entweder mit einer gezeichneten oder fotografierten Abbildung, bei der ein Körperteil an einen Sensor gehalten wird, oder mit einem abstrakten Symbol visualisiert. Manchmal gibt es auch Versuche, mit einem als primitive Strichzeichnung oder Comic-Bild angedeuteten Menschen diese Interaktion deutlicher einzubeziehen.[451] Der Mensch bleibt in den Darstellungen dabei meist dem System äußerlich. Er dient als Spender des Inputs, taucht weder in den anderen Rollen auf, in denen eine menschliche Entität (also auch eine Organisation oder als Personal) mit dem System interagiert, noch als jemand, an den sich die Konsequenzen der Systemausgabe richten. Dennoch sind gerade die Betroffenen, aber auch die anderen User bedeutende Adressatinnen der vereinfachten, erklärenden Bilddarstellungen. Kehren wir auf die Ebene der Mythen zurück, gilt es nämlich, diese insbesondere bei ihnen richtigzustellen:

> „Education of users is essential."[452]

4.3 Akteure

Doch wer sind die Nutzer genau, von deren Erziehung Roethenbaugh spricht? Über potentielle Kunden, die ein Fingerabdruckerkennungssystem erwerben, Administratorinnen und Betreuer des Systems bis hin zu tendenziell unfreiwillig Betroffenen fächert sich der Begriff des Users in ein breites Spektrum von Personen und Organisationen auf. Im Unterkapitel *User und Usees* (4.3.1) wird insbesondere die soziale Einordnung der betroffenen Personen im Verhältnis zum IT-System Biometrie betrachtet.

Der deutsche IT-Branchenverband Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) hat in Zusammenarbeit mit den Verbänden Bundesverband IT-Sicherheit e.V. (TeleTrusT) und Zentralverband Elektrotechnik-

[450] Vgl. ISO/IEC 2382-37:2017, S. 7.

[451] Als Comicfigur mit der Bildunterschrift „Subject presents biometric characteristic" bei Pato und Millett 2010, S. 2.

[452] Roethenbaugh 1998, Section 5.

und Elektronikindustrie e.V. (ZVEI) vor allem in den nuller Jahren aktive Öffentlichkeitsarbeit für die „deutsche Biometriewirtschaft“ betrieben.[453] Die »Landkarte Biometrie« umfasste 2008 74 kleine, mittelständische und große Unternehmen, die als Anbieter biometrischer Lösungen galten – in der Beratung oder Herstellung, als Integrator, Betreiber oder Vertreiber. Hiervon machten 43 komplett oder teilweise mit Produkten oder Dienstleistungen rund um Fingerabdruckbiometrie ihren Umsatz. Außerdem sind in der Publikation acht Forschungsinstitutionen, sechs Behörden, sieben Interessengruppen und zwei Diskussionsforen genannt, die zur deutschen „Biometrielandschaft“ gehören. Einige von ihnen und einige aus anderen Ländern sowie länderübergreifende werden im Unterkapitel *Zusammenschlüsse privater, öffentlicher und zivilgesellschaftlicher Akteure* (4.3.2) vorgestellt.

Schließlich werden im Unterkapitel *Normung und Harmonisierung* (4.3.3) wichtige Normungsgremien für die Industriestandards vorgestellt. Die Rechtsnormen bleiben außen vor – eine umfangreiche vergleichende Analyse mit Fokus auf Datenschutzaspekte hat hier Els J. Kindt vorgelegt.[454]

Die Auswahl der Akteure in diesem Kapitel ist deutlich beschränkt. Es soll lediglich darum gehen, einen Einblick in die enge Verzahnung von Industrie und Forschung geben, die deutlich macht, dass die informatische Biometrie eher Wirtschaftszweig als Wissenschaft ist.

4.3.1 User und Usees

Betroffene als *Usees*

Im Machtgefüge der menschlichen Akteure sind die betroffenen Personen die schwächste Gruppe. Sie sind diejenigen, die die Systeme benutzen *müssen*, aber nicht zwangsläufig benutzen wollen.

Der Begriff *Usee* ist für sie weitaus besser geeignet als *User*. Er verdeutlicht im Englischen sehr gut die passive Rolle, in der jemand nicht die Technik nutzt, benutzt oder anwendet, sondern zu einem von und mit der Technik benutzten Objekt wird. Der Begriff hat sich in den letzten Jahren kaum verbreitet.[455] Die Informatikerin Simone

[453] Siehe BITKOM e.V. 2008 sowie BITKOM e. V., TeleTrusT e. V. und ZVEI e. V. 2008.

[454] Siehe Kindt 2013.

[455] Unter Sozialwissenschaftlerinnen scheint er bisher unbekannt zu sein. Auf interdisziplinären, internationalen Konferenzen wie der „Security, Ethics, and Justice“, Juni 2012 in Tübingen, des Projekts KRETA (Körperscanner: Reflexion der Ethik auf Technik und Anwendungskontexte) oder der Konferenz „Digitale Praktiken“, Februar 2015 in Frankfurt/Main, kannten die Vertreterinnen der *Science and Technology Studies* den Begriff nicht. Auf ersterer wurde er dankbar aufgenommen, nachdem in einer Diskussion konstatiert wurde, es gebe eigentlich keinen Begriff für diese machtlose Nutzerinnengruppe. Wolfgang Coy hat mich darauf hingewiesen, dass der Begriff bereits auf einer Weltkonferenz der *International Federation for Information Processing* (IFIP) Ende der 1980er zur Diskussion stand. *Opfer* oder *Benutzte* würden im Deutschen aber besser passen.

Fischer-Hübner erwähnt ihn recht selbstverständlich mehrfach in ihrem Buch »IT-Security and Privacy«. Gleich in der Einführung benennt sie „data subjects [...] that are not necessarily acting as system users at the same time (e.g., bank customers, patients)“ mit „the so called usees“ und ergänzt:

> „A usee is a person about whom the IT-System produces and processes data, and who has usually no control over this process[.]“[456]
> „Unfortunately, usees normally do not participate in the system design process and consequently their privacy interests are often neglected.“[457]

Im Englischen drückt der Begriff das Machtgefälle, das im Vergleich zu freiwilligen Nutzerinnen in einem Szenario mit Kontrolltechnologien entsteht, geeignet aus, da dort das Suffix „-ee“ für Personen verwendet wird, die als Objekte, Empfänger oder Betroffene bestimmter Aktionen auftreten.

Data subject als alternativer Begriff, der sich sowohl im Vokabular englischsprachiger Datenschutzregularien findet als auch speziell in der Biometrie genutzt wird,[458] ist bezüglich des Ausgeliefertseins des zum Objekt gemachten „Subjekts“ zu neutral. Der in der Sprechweise deutscher Datenschutzregularien und im Rechtsjargon gebräuchliche Ausdruck *Betroffene* oder *betroffene Person* ist demgegenüber passender und wird in dieser Arbeit synonym mit Usee verwendet.

Erziehung, Gebrauchstauglichkeit und Rechtmäßigkeit

Roethenbaugh nennt zwei Hauptgründe für die Bedeutung der Ausbildung der Nutzerinnen in Hinblick auf biometrische Systeme:

> „Firstly, education helps to allay fears about data protection and privacy. Secondly, education is necessary to assist end users in the way they interact with a biometric system. Humans react differently when faced with technology and education can guide users and improve the overall performance of any application.“[459]

Eines der größten Probleme, mit dem sich die Disziplin und der Industriezweig der Biometrie konfrontiert sehen, sind die Datenschutzbedenken bezüglich der Nutzung von Biometrie: „the image of Big Brother is difficult to shrug off.“[460] Auch Bolle et al. stellen fest:

---

[456] Fischer-Hübner 2001, S. 3.

[457] Ebd., S. 32.

[458] Siehe zum Terminus *Biometric Data Subject* die kurzen Ausführungen im *Unterkapitel 2.2.4 Rollen der Interaktion von Mensch und Biometrie-System* (S. 37).

[459] Roethenbaugh 1998, Section 5.

[460] Ebd., Section 5.

> „Many people are afraid that biometrics, with its promise of perfect identification, inherently means a 'Big-Brotherish' complete erosion of privacy."[461]

Auch Dunstone/Yager bringen eine gefühlte breite Ablehnung einer allgemeinen Öffentlichkeit zur Sprache:

> „Biometrics also had problems with public perception in the post 9-11 world. In particular, it is commonly being seen as a big brother technology, potentially leading to the invasion of privacy."[462]

Das Motiv einer falschen „Big-Brother-Vorstellung" von Biometrie taucht in verschiedenen Publikationen der informatischen Biometrie immer wieder auf.[463] Dunstone/Yager und Roethenbaugh benennen als Akteure einer solchen Ablehnung vor allem „civil liberty and consumer groups" bzw. „civil libertarian pressure groups". Gerade durch die schnelle Ausbreitung der Biometrie in alle Lebensbereiche könnten solche Gruppen diese Ängste noch bestärken, denn:

> „The concept of a biometric national identity card, for example, is a little unsettling if the full picture is not made clear."[464]

Der Kritik, dass die Einführung biometrischer Anwendungen sehr schnell gegangen sei, ohne dass es eine öffentliche Debatte oder parlamentarische Beteiligung gegeben habe, wie sie beispielsweise der Rechtswissenschaftler Hornung in Bezug auf europäische Biometriepolitik formuliert hat,[465] wird ein Gegendiskurs entgegengesetzt werden:

> „Fears about a global Big Brother will be dismissed if end users are educated about the workings and purpose of the biometric system. It is important to stress the positive role played by such an environment of communication."[466]

Es sei zwar nicht auszuschließen, dass biometrische Systeme in totalitären Systemen zu Überwachungszwecken gebraucht werden könnten, aber bei richtiger politischer und rechtlicher Begleitung ließe sich dies verhindern, schreiben Bolle et al. Sie weisen sowohl die Vorstellung, dass biometrische Systeme keine Bedrohung der Privatsphäre darstellten als auch die, dass dem so sei, ins Reich des Mythen. Denn es komme auf den politischen Umgang damit an – in gewisser Weise weisen sie damit auch die Ver-

---

[461] Bolle u. a. 2004, S. 153.

[462] Dunstone und Yager 2009, S. 10.

[463] So auch bei Prabhakar und Bjorn 2008, S. 479, Yau 2009, S. 523.

[464] Roethenbaugh 1998, Section 5.

[465] Vgl. G. Hornung 2007, S. 246.

[466] Roethenbaugh 1998, Section 5.

antwortung von sich: „Privacy is a policy matter."[467] Politik, für die es bei zu schneller Einführung einer Technik eben wenig Zeit gibt.

Ein weiteres in der Fachliteratur auftauchendes Argument, das allzu starke Skepsis hinsichtlich der Datenschutzgefährdung durch die Biometrie zurückweisen soll, ist, dass – ein gutes Systemdesign mit wohlbedachten Haftungsprozeduren vorausgesetzt – Biometrie sogar für den Schutz der Privatsphäre geeignet sei.[468] Genannt werden beispielsweise die Möglichkeit einer besseren Rückverfolgbarkeit medizinischer Akten mittels Biometrie (wie genau, wird nicht erklärt) oder die Nutzung biometrischer Daten anstatt persönlicher Informationen wie der Sozialversicherungsnummer, der Adresse oder des Geburtsnamens der Mutter.[469] Interessant ist hier, dass biometrische Daten offenbar nicht als persönliche Informationen betrachtet werden, obwohl sie doch gleichzeitig das persönlichste darstellen, was wir von unserer Identität zu geben haben.[470] In Kombination mit Verschlüsselung könne man Biometrie auch als perfektes Datenschutzwerkzeug in verteilten Datenbanken verwenden, so Roethenbaugh.[471] Auch eine medizinische Diagnose sei mit biometrischen Daten nicht möglich, denn „biometric systems are not designed for this purpose",[472] und die mathematischen Codes, mit denen die einzigartigen Features gespeichert werden, seien ja eben keine Verhaltens- oder Körperprofile. Auch hier müsse man die User aufklären.[473] An dieser Stelle wird besonders deutlich, dass Erziehung und Aufklärung hier vor allem bedeuten, nur die positivistische Setzung dessen zu glauben, was die Technik tun soll und was alle mit ihr interagierenden Personen tun sollen, und nicht zu fragen, welche Potentiale sie bietet, wenn sie eben nicht wie gewünscht funktioniert oder genutzt wird. Es geht bei diesem Bildungsansatz vor allem darum, eine Deutungshoheit darüber zu behalten, wofür ein biometrisches System gut ist. Hierzu wird unterstellt, dass die Nutzer die Funktionsweise biometrischer Systeme nicht richtig verstehen, wenn sie sich vorstellen können, dass sie auch für Zwecke genutzt werden könnte, für die sie offiziell nicht entworfen wurde.

Jenseits von Erziehung gibt es den grundsätzlichen Appell an eine adäquate Gebrauchstauglichkeit der Systeme.[474] Zwar sehen Nutzerinnen sicher gern ein, dass biometrische Technologien in einem Hochsicherheitsszenario (Roethenbaugh nennt

---

[467] Bolle u. a. 2004, S. 153.

[468] Vgl. ebd. Roethenbough schlägt in die gleiche Kerbe: „Biometric technologies are a privacy protection tool rather than an infringement of civil liberties." (Roethenbaugh 1998, Section 5).

[469] Vgl. Bolle u. a. 2004, S. 153.

[470] Siehe hierzu *Unterkapitel 3.5.1 Identitätsbegriff* (S. 120).

[471] Vgl. Roethenbaugh 1998, Section 5.

[472] Ebd., Section 5.

[473] Vgl. ebd., Section 5.

[474] Vgl. ebd., Section 5.

hier Atomreaktoren als Beispiel) durchaus etwas zudringlicher sein dürfen. Dennoch sollten die Hersteller so gut als möglich zum Wohle aller auf nutzerfreundliche und leicht mit bestehenden Techniken integrierbare Systeme achten.

Jenseits aller Nutzerfreundlichkeit und wohlgemeinter Aufklärung bleibt am Ende jedoch eine normative Geste nicht aus: „The use of biometrics is, so far, permitted by law".[475] Die Rechtmäßigkeit des Einsatzes biometrischer Technik ergebe sich daraus, dass sie bisher nicht erfolgreich rechtlich bekämpft werden konnte. Roethenbaugh verweist in diesem Zusammenhang auf eine Zusammenstellung des Politikwissenschaftlers Kenneth P. Nuger, die dies belege – leider ohne Quellenangabe. Nuger hat beispielsweise zusammen mit Wayman untersucht, inwieweit Biometrie mit den Konzepten des Rechts auf ein rechtsstaatliches Verfahren („due process"), auf Privatsphäre („the right of privacy") sowie auf Schutz vor unverhältnismäßiger Durchsuchung und Beschlagnahmung („security from unreasonable search and seizure") in der Verfassung der Vereinigten Staaten vereinbar sei. Sie untersuchen hierfür auch für die Biometrie relevante Gerichtsverfahren.[476] Die Autoren kommen nach ihrer Analyse zu dem Schluss:

> „In a democracy, power ultimately rests with the people, and if the people ultimately feel threatened by biometric technologies, they certainly have the collective power to carefully modify, or even stop, its use in even reasonable situations."[477]

Außerdem formulieren sie politische Anforderungen für die Einführung biometrischer Technologien im öffentlichen Sektor, von deren Einhaltung sie sich auch ein wachsendes Vertrauen sowohl in die Technik als auch in die Regierung versprechen:

> „The higher the social trust in government,which is currently at record low levels, the greater will be the chance of both the public and legal acceptance of this emerging technology into our society."[478]

Die fünf Anforderungen umfassen folgende Punkte:[479]

1. die prinzipielle Möglichkeit, sich rechtlich gegen nachteilige biometrische Entscheidungen zu wehren und damit, gesetzlich gesichert, die Fehlbarkeit von Biometrie anzuerkennen,

2. keine unbemerkte Vermessung biometrischer Charakteristika etwa durch heimliche Nutzung latenter Fingerabdrücke,

[475] Roethenbaugh 1998, Section 5.

[476] Vgl. Nuger und Wayman 2005.

[477] Ebd., S. 328.

[478] Ebd., S. 329.

[479] Vgl. ebd., S. 328 f.

3. Datensparsamkeit und enge Zweckbindung,
4. keine Nutzung der Daten in anderen als den angegebenen Kontexten und keine Weitergabe an andere Institutionen,
5. Absicherung der Korrektheit der gesammelten Informationen.

User und Automatisierung

Nach rechtlicher und politischer Vermittlung innerhalb der gesellschaftlichen Sphäre wird häufig dann verlangt, wenn es um die Probleme biometrischer Techniken geht. Der Mensch und seine Institutionen sollen dann in einem vermeintlichen Mensch-Maschine-Gegensatz vermitteln.

So stellen Nuger und Wayman „Privacy Versus Security“ mit dem Gegensatzpaar „Mankind Versus Machine“ auf eine Stufe.[480] Erst in der modernen, urbanen, anonymen Gesellschaft entstünden die Kontrollinstrumente zur Wahrung einer gesellschaftlichen Sicherheit, die das als etwas Neues hinzugewonnene Anonyme eingrenzen und kontrollierbar halten sollten, das gleichermaßen Gefahr und als Privates Privileg bedeute. Die Mittel, die das Private schützen sollten, bedrohten es aber wiederum ebenfalls. Die Maschinisierung der statistischen Kontrolle, die automatische Verknüpfung von Individuen und beliebig konstruierbaren Handlungen setzten nun offenbar der Idee individueller Kontrolle menschlichen Handelns vollends ein Ende. Die mit dem Gegensatzpaar beschriebenen Spannungen sind dialektischer Natur insofern, als dass diese Gegensätze einander bedingen und durch verfassungsrechtliche Instrumente in einer Balance gehalten werden müssen. Den Nutzerinnen der Technik kommt in dieser Sicht am Ende die Handlungshoheit zu, da sie diese Instrumente steuern und in ihrem eigenen Interesse steuern müssen.

Auch auf viel praktischeren Ebenen muss der Mensch die Unzulänglichkeiten der Automatisierung kompensieren. So heißt es in den Ausführungen Waymans zum Terminus „automatisiert“, dass sein Eingriff vor allem bei maschinellen Fehlern wichtig werde:

> „The automatic pattern matching is always probabilistic and so decisions are always made with some level of uncertainty. Errors are made by these technologies. In applications where a machine error can result in the denial of service to a user, a method for human adjudication is always available. Human intervention for exception handling is within the definition of biometric authentication.“[481]

Das Wechselspiel gegenseitiger Fehlerbehebung wird deutlich: Die Fehler, die der Mensch bei einer Erkennung macht, soll die Maschine ausgleichen. Die Fehler, die die

[480] Vgl. ebd., S. 311.

[481] Wayman 1998, S. 21.

Maschine wiederum beim Erkennen oder als prinzipielle Fehlfunktion erzeugt, muss aber wiederum der Mensch beheben usf. Biometrie ist insofern eine Teilautomatisierung des sozialen Vorgangs des Erkennens, die dessen Fehlerdimensionen erweitert, aber die User nahezu komplett dafür in die Verantwortung nimmt.

4.3.2 Zusammenschlüsse privater, öffentlicher und zivilgesellschaftlicher Akteure

Die informatische Biometrie ist von Anfang an durch Multi-Stakeholder-Kooperationen aus staatlichen Behörden, Normungsinstitutionen, Wissenschaft, Forschung, Industrie sowie teilweise einbezogenen zivilgesellschaftlichen Organisationen geprägt, die sich in zahlreichen Konferenzen und Workshops vernetzen. Viele Zusammenhänge sind dabei sehr dynamisch, ihr „Label" existiert nur wenige Jahre und die darunter gruppierten Firmen, Universitäten, Forschungsinstitute, Behörden und Berufsverbände finden sich später wieder unter neuem Namen in einem ähnlichen Netzwerk zusammen.

Beispielhaft soll diese Mischung im Folgenden anhand des institutionellen Netzwerks der alljährlich anwachsenden Sponsoren und Mitorganisatoren der inzwischen seit mehr als zehn Jahren auch international etablierten und gut dokumentierten Konferenz der deutschen Fachgruppe »Biometrik und elektronische Signaturen« der Gesellschaft für Informatik e. V. (GI) (*Biometrics Special Interest Group*, BIOSIG) illustriert werden.

BIOSIG

Die Fachgruppe »Biometrik und elektronische Signaturen« ist Teil des im Jahr 2002 gegründeten Fachbereichs »Sicherheit« der GI und führt seit eben diesem Jahr alljährlich Workshops und ab 2003 die internationale Konferenz *Biometrics and Electronic Signatures* durch, von der anfangs zunächst unregelmäßig offizielle Proceedings erschienen.[482] Sie sieht sich „als fachliches Diskussionsforum für Wissenschaftler, Entwickler, Anwender und Vertreter von Aufsichtsstellen und Regulierungsbehörden" inzwischen vor allem in den Bereichen „Biometrie und Identitätsmanagement".[483]

Das Fraunhofer-Institut für Graphische Datenverarbeitung (Fraunhofer IGD) spielt eine tragende Rolle in der Fachgruppe und ist von Anfang an Gastgeber der internationalen Konferenz.

[482] Die Konferenzbeiträge sind umfangreich dokumentiert: siehe Brömme und Busch 2003, Brömme, Busch und Hühnlein 2007, Brömme, Busch und Hühnlein 2008, Brömme, Busch und Hühnlein 2009, Brömme und Busch 2010, Brömme und Busch 2011, Brömme und Busch 2012, Brömme und Busch 2013, Brömme und Busch 2014, Brömme, Busch, Rathgeb u. a. 2015 und Brömme, Busch, Rathgeb u. a. 2016. Ein erster Workshop unter diesem Namen fand allerdings bereits 2002 statt – die Veranstalter zählen diesen aber in der Konferenzbandreihe anscheinend nicht mit (siehe bspw. Borchers 2003).

[483] http://fg-biosig.gi.de, letzter Abruf: 29.7.2017.

CAST e.V.

Die BIOSIG-Konferenz des ersten Jahres wurde zunächst lediglich von der Fachgruppe und dem *Competence Center for Applied Security Technology* (CAST) veranstaltet, das bis heute als unterstützender Verein dabei ist. In der Hochphase der Einführung biometrischer Ausweise und Pässe in Europa ging es vor allem um die Unterstützung der internationalen Standardisierung.

CAST zählt inzwischen „251 Mitglieder aus Wissenschaft, Industrie und Öffentlichem Dienst“.[484] Sein Sitz ist wie der des Fraunhofer IGD in Darmstadt. Es bietet für Studierende und Berufstätige Weiterbildungsprogramme an, vergibt Förderpreise für akademische Qualifikationsarbeiten und arbeitet beratend im Bereich der IT-Sicherheit.

BSI

Im Jahr 2004 stieg das BSI als Mitveranstalter in die Konferenz ein, trug aber bereits in den ersten Veranstaltungen inhaltlich durch Referentinnen dazu bei.

Für die deutsche Biometrie spielt das 1991 gegründete und zum Bundesministerium des Innern gehörende BSI eine Schlüsselrolle. Es prüft, zertifiziert und akkreditiert die bei den Behörden eingesetzten biometrischen Techniken und hat öffentlichkeitswirksame Studien zur Effektivität u. a. von Fingerbiometrie durchgeführt und so erheblich zur Legitimation der Technik in Deutschland beigetragen.[485] Zudem bietet es umfangreiche Hintergrundinformationen zum Thema Biometrie auf seiner Webseite an.

Außerdem hat es 2002 und 2004 selbst zwei Biometrie-Symposien veranstaltet, auf dem 2004 James L. Wayman ein Award „in Anerkennung seines Lebenswerkes und seines Einsatzes für eine Biometrie, die gegenüber den juristischen und sozialen Aspekte[n] der Technik nicht blind ist“, verliehen wurde.[486]

3D Face Research Consortium

Zwischen 2006 und 2008 trat zu den bisher genannten Akteuren, die als Veranstalter der BIOSIG-Konferenz auftauchen, das *3D Face Research Consortium* hinzu. Es war ein im Rahmen des 6. Rahmenprogramms für Forschung und technologische Entwicklung (*Framework Programme for Research and Technological Development*, FP6) für knapp drei Jahre mit mehr als 6,5 Millionen Euro gefördertes Projekt.[487] Geforscht wurde über dreidimensionale Gesichtserkennungstechniken, deren Verbindung mit zweidimensionalen Techniken sowie deren Einsatz in Hochsicherheitsumgebungen.

---

[484] https://www.cast-forum.de/mitglieder/cast.html, letzter Abruf: 29.7.2017.

[485] Dazu gehören die Studien von BSI, BKA und IGD 2008 oder auch BSI 2005, die zusammen mit dem BKA und dem Fraunhofer IGD bzw. der Firma Secunet durchgeführt wurden.

[486] Borchers und Kuri 2004.

[487] CORDIS 2008a. Die Gesamtkosten des Projekts wurden mit knapp 12 Millionen veranschlagt.

Federführend war die französische Firma Sagem Sécurité S.A. (heute: Morpho). Aus Deutschland waren mit der Bundesdruckerei GmbH, dem BKA, den Firmen Cognitec Systems GmbH, Flughafen Berlin-Schönefeld GmbH, L-1 Identity Solutions, Polygen Technology GmbH, dem Zentrum für Graphische Datenverarbeitung E.V. sowie der Fraunhofer Gesellschaft die meisten Unternehmen und Organisationen beteiligt.

European Biometrics Forum (EBF)

Das *European Biometrics Forum* (EBF), das im Jahr 2009 einmalig als Mitunterstützer der BIOSIG-Konferenz auftauchte, existiert seit 2011 nicht mehr. Denn es war ein typisches organisatorisches Kurzzeitkonstrukt eines Multi-Stakeholder-Verbandes, wie er schon nach wenigen Jahren wieder verschwindet. Verfolgt man über mehrere Jahre den Biometriediskurs, stellt man leicht fest, dass Webseiten großer und schlagkräftig erscheinender Industrie-Wissenschaft-Politik-Kooperationen nach zwei bis sechs Jahren wieder verschwinden. Das sind in der Regel Perioden, die den Förderphasen bestimmter öffentlicher Forschungsprogramme entsprechen. Oft werden sie von denselben Schlüsselpersonen in ähnliche Netzwerke mit neuem Namen überführt – eine in einer projektgesteuerten Forschungslandschaft ganz übliche, nicht biometrie-spezifische Praxis.

Das EBF entstand Ende 2002 aus dem BioVisioN-Projekt heraus, das mit Mitteln des 5. EU-Forschungsrahmenprogramms ein Jahr lang mit knapp 400.000 Euro gefördert wurde. Dessen Ziel war es, einen Fahrplan für die Entwicklung der europäischen Biometrie in den kommenden zehn Jahren zu entwerfen unter der Maßgabe ihrer sicheren, nutzerfreundlichen, sozial akzeptablen und ethisch vertretbaren Nutzung. Hierfür sollte ein Europäisches Biometrie Forum etabliert werden, das die Bedürfnisse einer „European biometrics community" abbildet.[488] Die neun Projektteilnehmer aus Großbritannien (BTexact Technologies Ltd., Nationwide Building Society, Government Communications Headquarters/Communications Electronic Securities Group, NPL), Irland (Daon Ltd.), Deutschland (Fachhochschule Gießen-Friedberg, TeleTrusT), Italien (Consiglio Nazionale delle Ricerche) und den Niederlanden (Stichting Centrum voor Wiskunde en Informatica) waren die entscheidenden Initiatoren.

EU JRC

Außerdem taucht seit 2009 das *Joint Research Centre of the European Commission* (JRC) der Europäischen Kommission, ein Generaldirektorat der EU, als Förderer von BIOSIG-Konferenzen auf. Die Gemeinsame Forschungsstelle der Europäischen Kommission ist ein wissenschaftlicher Dienst mit mehreren Forschungsinstituten. Im Bereich Biometrie hat sie diverse Studien unterschiedlicher Natur durchgeführt oder beauftragt.[489]

[488] CORDIS 2005.

[489] Bspw. Maghiros u. a. 2005 (*Institute for Prospective Technological Studies*), Waggett 2015 (*Institute for the Protection and Security of the Citizen*) oder die Studien FRONTEX 2007 sowie FRONTEX 2010.

CASED

Das *Center for Advanced Security Research Darmstadt* (CASED) war ein Kooperationsprojekt der »Projektgruppe verfassungsverträgliche Technikgestaltung« (provet) des Instituts für Wirtschaftsrecht der Universität Kassel, der TU Darmstadt, des Fraunhofer SIT sowie der Hochschule Darmstadt und wurde im Rahmen der Landes-Offensive zur Entwicklung wissenschaftlich-ökonomischer Exzellenz (LOEWE) des Landes Hessen gefördert.[490] In ihm haben Juristinnen und Informatikerinnen zusammengearbeitet.

Biometrics European Stakeholders Network (BEST Network)

Ab 2010 verbreitert sich das Sponsoren- und Organisatoren-Team der BIOSIG-Konferenz weiter. Nun taucht das *BEST Network* als Veranstalter mit auf – ebenfalls ein kurzlebiger, an den EU-Forschungsprogrammen ausgerichteter Zusammenhang.

Im März 2010 wurde die Website des aus Mitteln des 7. Forschungsrahmenprogramms (2007–2013) der Europäischen Kommission, Themenbereich »Informations- und Kommunikationstechnologien«, geförderten Netzwerks online geschaltet und war bis ca. Mitte 2014 verfügbar.[491] Nach Eigendarstellung sollte das Netzwerk einen europäischen Austausch über „trusted information infrastructures and biometric technologies“ zwischen und mit „key stakeholders including the finest experts from across the EU“ ermöglichen, um zu ermitteln, „how biometrics can most appropriately be applied“.[492] Es sollten vor allem auch Informationen über erste praktische Erfahrungen mit Pilotprojekten und real genutzten Systemen länderübergreifend ausgetauscht werden. Ein wichtiges Ziel wurde so formuliert:

> „Recent experiences with biometrics-enabled systems and services have revealed issues beyond accuracy of identification that would need to be addressed in a holistic approach. These include the usability of biometric technologies, user preferences, protecting the privacy of citizens and ensuring full inclusiveness for all users of such systems.“[493]

Auch Werkzeuge zur besseren Abschätzung der Wirtschaftlichkeit von Biometrieprojekten sowie verbesserte Implementationsrichtlinien sollten entstehen. Schwerpunkte

---

[490] http://www.uni-kassel.de/fb07/institute/iwr/personen-fachgebiete/rossnagel-prof-dr/forschung/provet/cased.html, letzter Abruf: 29.7.2017.

[491] Die Domain http://www.best-nw.eu/ wurde bei *archive.org* das letzte Mal am 21.8.14 archiviert: https://web.archive.org/web/20140821080128/http://www.best-nw.eu, letzter Abruf: 28.7.2017. Die letzte dort verzeichnete offizielle Aktivität war eine Konferenz am 17. Februar 2012 in Brüssel.

[492] Nach der Eigenbeschreibung auf der in der letzten Fußnote genannten Webseite.

[493] CORDIS 2017.

waren „visa, passport and border control applications, as well as of future development including evolving applications such as eID and electronic services.“[494]

Hierzu arbeiteten mehr als 20 Organisationen und Unternehmen in den sieben Arbeitsgruppen »Border Control and Immigration«, »Emerging applications«, »European Registered Travellers schemes«, »Biometrics and e-ID«, »Training & Education«, »Testing & Certification« und »Ethical, Legal and Socio-technical aspects« zusammen. Das Projekt wurde nach dem Fördermodell »Thematische Netzwerke« mit 478.000,- Euro vom 1.10.2009 bis 31.3.2012 gefördert – einem Modell, bei dem die Koordinierungskosten des Netzwerks mit pauschal 2000,- bis 3.000,- Euro pro Jahr für maximal 20 Beteiligte und für alle Beteiligten mit pauschal 5.000,- Euro pro Jahr für Konferenz- und Reisekosten finanziert werden.[495]

Aus dem Netzwerk heraus wurden einige interessante Dokumente als Ergebnisse veröffentlicht, die in bestimmten Bereichen einen guten Überblick über Zertifizierungs- oder Trainingsprogramme, genutzte Standards für Biometrietechnologien, typische Kritiken und ethische Bedenken in verschiedenen EU-Staaten im Projektzeitraum bieten und über den Informationsdienst *Community Research and Development Information Service* (CORDIS) zumindest teilweise weiter verfügbar sind.[496]

Die Beteiligten waren hier:

- Forschungs- und Bildungsinstitutionen:
  - Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung e.V.,
  - Technische Universität Graz,
  - Universidad Carlos III de Madrid,
  - Institut Mines-Télécom (Frankreich),
  - University of Kent,
  - University of Leeds,
  - Centre for Research and Technology Hellas,
  - Centre for Science, Society and Citizenship (Italien),
  - Universita degli Studi Roma III,
  - Stichting Katholieke Universiteit Brabant/Universiteit van Tilburg,
  - Universiteit Twente (Niederlande),
  - Hochschule Gjøvik (Norwegen),

[494] CORDIS 2017.

[495] Vgl. DG Information Society and Media, European Commission 2008.

[496] Vgl. CORDIS 2017. Auf der Webseite zum Projekt sind Projektpublikationen unter »Documents and Publications« hinterlegt.

- Industrie/Privatwirtschaft:
  - Secunet Security Networks AG (Deutschland),
  - Morpho S.A.S. (Frankreich),
  - Daon, Inc. (Irland),
  - Fujitsu Services Ltd. (UK),
  - Schiphol Nederland B.V.,
- Öffentliche Institution für Datenschutz:
  - Unabhängiges Landeszentrum für Datenschutz (ULD),
- Lobby-/Beratungsinstitute; öffentlich-private Interessengruppen:
  - EUROSMART AISBL (Brüssel),
  - Ancitel S.p.A. (Italien),
  - RAND Europe Community Interest Company (UK),
  - Association BioSecure (Frankreich),
  - European Biometrics Group (Niederlande),
  - NPL Management Limited (UK).

TeleTrusT/BITKOM

Seit 2010 unterstützt auch TeleTrusT offiziell die BIOSIG-Konferenz. Der Branchenverband TeleTrusT ist ähnlich wie BITKOM insbesondere seit den nuller Jahren sehr um die Förderung der deutschen Biometrie bemüht.
TeleTrusT versteht sich als „Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst.“[497] Die Biometrie-AG des Verbandes trifft sich mehrmals jährlich in Berlin und in Darmstadt, lädt Gäste aus Industrie und Forschung ein und ist dabei offen für interessierte Gäste.

Weitere

Schließlich sind innerhalb der letzten fünf Jahre noch die *European Association for Biometrics* (EAB), das *Norwegian Biometrics Laboratory* (NBL), der *IEEE Biometrics Council*, die *ICT COST Action IC1106* sowie die *Institution of Engineering and Technology* (IET) hinzugestoßen.

[497] https://www.teletrust.de/ueber-teletrust/ziele-und-nutzen, letzter Abruf: 28.7.2017.

4.3.3 Normung und Harmonisierung

Kurze Zeit nachdem Ende 2001 in den USA innerhalb des INCITS ein neues Technisches Komitee für Biometrie gegründet worden war, nahm das ebenfalls von den USA vorgeschlagene *Subcommittee 37 »Biometrics«* (SC37) mit Vertreterinnen unterschiedlicher Institutionen aus Wissenschaft und Industrie und aus 17 verschiedenen Nationen seine Arbeit auf.[498] Es besteht aus sechs Arbeitsgruppen:

1. *Working Group 1* (WG 1) – »Harmonized Biometric Vocabulary«,
2. *Working Group 2* (WG 2) – »Biometric Technical Interfaces«,
3. *Working Group 3* (WG 3) – »Biometric Data Interchange Formats«,
4. *Working Group 4* (WG 4) – »Biometric Profiles«,
5. *Working Group 5* (WG 5) – »Biometric Performance Testing and Reporting«,
6. *Working Group 6* (WG 6) – »Cross-Jurisdictional and Societal Aspects of Biometrics«.

Die für eine gemeinsame begriffliche und modellbildende Basis wichtige Arbeit der WG 1 griff vor allem auf Vorarbeiten des *Biometric Consortium* sowie des *National Biometric Test Center* in den 1990er Jahren zurück:

> „The scientific agenda for the National Biometric Test Center was established by the Biometric Consortium in the 1995 Request for Proposal and in a series of questions posed at that time to the community by the Consortium Chair, Dr. Joseph P. Campbell. Why have biometric device tests failed to adequately predict 'real-world(s)' performance? What operational factors affect error rates? Should testing results be reported as ROC curves or as rank order statistics? How big should tests be and can confidence intervals be placed on test outcomes?"[499]

Internationale Standards waren nötig, um Antworten für diese die Systemfehler biometrischer Systeme betreffenden Fragen verbindlich festzulegen.

Die Standardisierungsbestrebungen auf internationaler Ebene, die eine globale Vermarktung der Sicherheitstechnologien, die internationale Kooperation der Polizeien und globale Kontrolle von Migrationsbewegungen ermöglichen, wurden angestoßen von NIST und ANSI mit Rückgriff auf die jahrzehntelangen Vorarbeiten des FBI. Insbesondere für die nötigen Standardisierungen der Biometrie im internationalen Reiseverkehr übernahm die *International Civil Aviation Organization* (ICAO) eine tragende Rolle. Über verschiedene große Kooperationen von Staat, Wissenschaft und Wirtschaft, wie sie für die europäische Ebene im *Unterkapitel 4.3.2 Zusammenschlüsse privater,*

[498] Vgl. Tilton 2011, S. 1.

[499] Wayman 2000, S. iii.

öffentlicher und zivilgesellschaftlicher Akteure (S. 158) beschrieben wurden, koordinieren sich die Interessengruppen bei ISO und ICAO.

Das SC37 trifft sich einmal jährlich in einer Plenarsitzung. Es besteht seit 2002 und hat mit Stand Ende 2013 „insgesamt 86 Dokumente (Biometrie-Standards und *Technical Reports*) erarbeitet und veröffentlicht. Darüber hinaus befinden sich 60 Projekte in Erarbeitung."[500] Inzwischen sind 28 Nationen mit ihren jeweiligen Normungsinstitutionen als Mitglieder vertreten. Deutschland beteiligt sich beispielsweise mit dem privatwirtschaftlich getragenen Verein Deutsches Institut für Normung (DIN), der mittels des Deutschen Normenvertrags von 1975 die einzige staatlich autorisierte nationale Institution für Standardisierung ist. Im DIN ist der Normenausschuss Informationstechnik und Anwendungen (NIA) 043-01-37 „das deutsche Spiegelgremium des internationalen Normungskomitees ISO/IEC JTC 1/SC 37 ‚Biometrics'."[501] Auf europäischer Ebene wiederum gibt es im *Technical Committee 224 »Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment«* des *Comité Européen de Normalisation /European Committee for Standardization* (CEN) die *Working Group 18 »Biometrics«*.

4.4 Fazit

In den wenigsten der vorgestellten Diskursfelder werden Sinn und Zweck sowie ethische Vertretbarkeit biometrischer Erkennung grundsätzlich in Frage gestellt. Es geht in der Regel um einen angemessenen Einsatz je nach Szenario oder vielleicht bezogen auf eine konkrete Anwendung auch um einen punktuellen Verzicht. Die grundsätzliche Ablehnung automatischer Personenerkennung wird nicht offen verhandelt. Doch dies lohnt sich auf zweierlei Weise. Erstens kann vermieden werden, dass die Fixierung auf eine Algorithmisierung eines möglicherweise genuin zwischenmenschlichen Problems den Blick dafür verstellt, welche sozialen Funktionen das Einander-Erkennen eigentlich hat. Zweitens gewinnen dann gesellschaftliche Aushandlungsprozesse bei damit einhergehenden sozialen Problemen – Verbindlichkeit einer Erkennung, das Vertrauen darin, wer jemand behauptet zu sein und die damit verbundene gegenseitige Verantwortung für die daraus folgenden Handlungen, Zuwendungen oder Ablehnungen – wieder an Bedeutung. Ihre Lösung wird sonst möglicherweise verlernt und einfach nur an technische Systeme weitergegeben, die sie aber genauso wenig lösen können, da sie der Unschärfe bedürfen. Beide Aspekte sind wohl kaum in zwei so harmlose Feststellungen zu zwängen. Sie sollen dennoch aus einer informatisch-philosophischen Sicht entgegen der reinen Machbarkeitslogik, Biometrie als originelles Modellierungsproblem der Mustererkennung zu betrachten, als Fazit dieses Kapitels diskutiert werden.

[500] TeleTrusT e. V. 2015, S. 19.

[501] http://www.din.de/de/mitwirken/normenausschuesse/nia/nationale-gremien/wdc-grem:din21:63278346, letzter Abruf: 29.7.2017.

4.4.1 Die „perspektivische Blindheit“ als grundlegender Entwurfsfehler

„›Blindheit‹ als durch den Vorsatz, programmieren zu wollen, geschaffenes Problem.“[502]

Einander zu erkennen ist eine Alltagshandlung, die sich nicht programmieren lässt. Ohne einen Identitätsbeweis zum Zeitpunkt der Erstregistrierung kann ein Fingerabdruckerkennungssystem komplett nutzlos werden.[503] Dass jemand wirklich die Person ist, die das System erkennt, muss zu irgendeinem Zeitpunkt von einem dem System äußerlichen Kontext bezeugt werden. Dass eine Identifikation richtig ist, wissen nur die Identifizierten selbst oder diejenigen, die eine Person kennen, die identifiziert wurde. In der Regel wird auch einem sogenannten Identitätsnachweis wie einem Ausweis oder ähnlichem vertraut, der jedoch ebenfalls einen solchen Kontext für seine Glaubwürdigkeit benötigt. Das Identifikationsparadox besteht darin, dass die mustererkennende Maschine nicht prüfen kann, ob die Muster wirklich einander hinreichend ähnlich sind oder ob sie einen Fehler gemacht hat.

Das Problem ähnelt dem Problem der „perspektivischen Blindheit“ in Expertensystemen, wie es Winograd und Flores vor allem in Rückgriff auf Heidegger beschreiben. Zwar ist das Wiedererkennen kein Gegenstandsgebrauch im Heideggerschen Sinne wie beim Hämmern: um zu hämmern, muss man nicht das Wesen des Hammers begreifen. Die Idee lässt sich aber transformieren. Flores und Winograd übertragen sie auf Künstliche Intelligenzen: Expertensysteme selbst wissen nicht, wann sie einen Gegenstand falsch oder richtig erkennen. Dieses Wissen kann ihnen auch nicht programmiert werden – es ist ein Urteil a priori, das vor der Analyse kommt. In Bezug auf biometrische Systeme bedeutet das: Um eine Person zu erkennen, muss man kein mechanistisches Wissen um die Prozesse, die im Körper, im Hirn oder in der Umgebung dabei ablaufen, haben. Der Mensch erkennt sie einfach. Vielleicht ist das nähere Nachdenken darüber, wieso wir jemanden erkennen, gar hinderlich: Denken Sie nur lange genug darüber nach, ob Sie wirklich Sie selbst sind oder Ihre Freundin wirklich Ihre Freundin oder aber vielleicht nur ein Klon Ihrer Freundin, sie begeben sich auf ein gefährliches Pflaster psychologischer Manipulation. Würde Sie dann die biometrische Erkennung Ihrer Freundin beruhigen? Das biometrische Merkmal wäre ja vielleicht auch perfekt geklont. Oder gehört sie zu dem geringen Prozentsatz der Menschen, bei denen die Maschine irrt. Und was, wenn die geklonte Freundin beteuert, dennoch dieselbe zu sein? Lügt sie dann nicht?

Das Spiel würde geradezu irrsinnig und im Alltag ist es dies glücklicherweise oft nicht. In dem ein oder anderen Kriminalfall mag und mochte es derartige Verwirrungen geben. Die Existenz der Daktyloskopie ist da ein dankbarer wissenschaftlich fundierter Rettungsanker, der lästige Diskussionen beendet. Sie stellt selbstverständlich nur

[502] Winograd und Flores 1992, S. 166.

[503] Siehe sowohl *Abschnitt: Grenzen der Aussagekraft statistischer Fehler* (S. 101) zur Frage der Herstellung einer Grundwahrheit sowie *Unterkapitel 3.5.1 Identitätsbegriff* (S. 120).

forensische Indizien und nicht Beweise zur Verfügung. Ohne Kontext des gesamten Settings wäre sie nicht allzu hilfreich. Dass biometrische Verfahren allerdings auch zur Verurteilung Unschuldiger führten, hat diese in der Regel dennoch kaum in Frage gestellt.

Nun lässt sich aber auch behaupten, wir nutzten alle schon „seit Menschengedenken" Biometrie, „wenn es um das Erkennen unserer Mitmenschen geht".[504] Da nun „ab einer gewissen Zahl" – von Menschen vermutlich – keine „zuverlässige Erkennung" mehr möglich sei, müssten biometrische Erkennungssysteme die Aufgabe des „*homo mensurans*" übernehmen.[505] Dieses Argument ähnelt dem, dass das menschliche Kurzzeitgedächtnis so etwas wie der Arbeitsspeicher ist und ist insofern interessant, als dass menschliche Verhaltensweisen mit maschineller Funktionalität gleichgesetzt werden – eine typische mechanistische Herangehensweise, die ebensowenig erklärt, wie der Rekurs auf Apriori-Wissen, der allerdings weniger verspricht.

Es ist sinnlos, menschliches Erkennen zu formalisieren. Was auch immer wir an menschlichem Erkennen formalisieren, in algorithmisierbare Teilprobleme zerlegen und mit Rückgriff auf stochastische Verfahren mit einer intuitiven Note zu versehen suchen, löst das Paradox nicht auf, dass es keine final verifizierbare Vergleichsinstanz für jemandes wahre Identität gibt. Nichtsdestotrotz glauben Fachleute aus dem Maschinellen Lernen daran, dass sie Umgebungen schaffen können, in denen dieser Bezug zu einem menschlichen Urteil gar nicht mehr nötig ist.

4.4.2 Sicherheitsdiskurs und sicherheits-industrieller Komplex

Biometrische Technologien sind Teil eines Sicherheitsdiskurses, in dem Sorgen, Angst oder Panik vor dem fremden Anderen und dem Kriminellen beruhigt werden müssen. Es ist dabei eine ganz selbstverständliche, beiläufig erwähnte, fast als allgemeine Wahrheit geltende Behauptung, dass Biometrie „unsere" Gesellschaft sicherer macht:

> „Consequently, biometrics is not only a fascinating pattern recognition research problem but, if carefully used, is an enabling technology with the potential to make our society safer, reduce fraud and provide user convenience (user friendly man-machine interface)."[506]

Die angeblich wachsende Gefahr des Identitätsbetrugs ist ein häufig auftauchendes Motiv in der Rechtfertigung zur Verbreitung der Alltagsbiometrie:

---

[504] Wiedemann 2012, S. 18.

[505] Ebd., Hervorhebung im Original. Der Begriff des *homo mensurans* ist von Haustein 2001, S. 3 übernommen, aber hier deutlich falsch verstanden: Er sieht den messenden Menschen als den Menschen der arbeitsteiligen Gesellschaft, der modernen industriellen Produktion, aber auch der Dienstleistungsgesellschaft. In diesem Sinne ist das Erkennen durch Messen eben gerade nicht das intuitive Erkennen.

[506] Maltoni u. a. 2009, S. 2.

> „More recently, however, increasing concerns about security and identity fraud have created a growing need for fingerprint and other biometric technologies for person recognition in a large number of non-forensic applications.“[507]

Noch schwammiger, aber in die gleiche Richtung zielend, ist eine Aussage wie diese:

> „At the beginning of the 21st century it has become increasingly clear that our information and communication systems infrastructure would be unable to achieve its full potential until methods of reliably verifying the identity of the individuals using that infrastructure can be developed. Biometrics in general, and fingerprint identification in particular, appears capable of this gap in the infrastructure.“[508]

Damit einher geht die Diskreditierung althergebrachter Identifizierungstechniken. Die Unterschrift etwa genießt im Allgemeinen sehr hohes Vertrauen, schon bei der Prüfung durch Augenschein. Für Biometrikerinnen aber ist sie von eher geringem Wert:

> „Signatures have been acceptable in government, legal, and commercial transactions as a method of verification for a long time. Signature is a behavioral biometric that changes over time and is influenced by physical and emotional conditions of the signatories. Signatures of some subjects vary a lot: even successive impressions of their signature are significantly different. Furthermore, professional forgers can reproduce signatures of others to fool the unskilled eye.“[509]

Nichtsdestotrotz gibt es auch für die automatisierte Unterschriftenerkennung Lösungen wie die vom Fraunhofer IGD, die eine Unterschriftenerkennung anhand der Schriftdynamik für Bankkarten entwickelt haben.[510] Die Prüfung durch Augenschein wird hier im Verhältnis zur maschinellen Prüfung als unsicher und ungeeignet dargestellt.

Die zivilgesellschaftliche Organisation *Statewatch* sieht die europäische Biometrie als Teil eines sicherheits-industriellen Komplexes,[511] die gestützt durch das *European Security Research Programme* einen enormen Aufschwung nehmen konnte, der kaum demokratischer Kontrolle unterlag. Jonathan P. Aus spricht konkret auf Eurodac bezogen von einem *Supranational Biometric Control Regime.*[512]

---

[507] Maltoni u. a. 2009, S. 1 f.

[508] Setlak 2004, S. 27.

[509] Maltoni u. a. 2009, S. 10.

[510] Vgl. Baier 2013.

[511] In der NeoConOpticon-Studie werden die EU-geförderten Biometrie-Forschungsprojekte der nuller Jahre aufgelistet und in diesen Kontext eingeordnet. Hayes stellt darin fest: „EU research funded to date assumes public consent to biometrics, with potential and tangible opposition reduced to ‘ethical concerns’.“ (Hayes 2009, S. 48).

[512] Vgl. Aus 2006, S. 5 ff.

Eine ganz besondere Rolle kam innerhalb des Sicherheitsdiskurses um Biometrie den Terroranschlägen vom 11. September 2001 in New York und Washington zu. Sie wurden zu *der* Formel für eine neue unsicherere Welt.

> „Some of the difficult problems in fingerprint recognition will entail solving not only the core pattern recognition challenges but also confronting some challenging system engineering issues related to security and privacy."[513]

Die Entwicklung der wissenschaftlichen Biometrie ist also eng verknüpft mit industriellen Interessen. Deutlich wird dies nicht zuletzt auch daran, dass wissenschaftliche Publikationen mit schwer überprüfbaren Fakten über den wirtschaftlichen Erfolg biometrischer Systeme unterfüttert werden.

Eine in der wissenschaftlichen Literatur und häufig in Fachkonferenzen zitierte Studie ist der »Biometrics Market and Industry Report« der *International Biometric Group*, die inzwischen zur *Novetta Solutions* gehört.[514] Der nicht-öffentliche Bericht kostete laut Pressemitteilung der Firma 3.995 Euro.[515]

Einen derart teuren und kaum überprüfbaren Bericht heranzuziehen, ist vor allem im Kontext vermeintlich wissenschaftlicher Fachliteratur erstaunlich. Beliebt ist vor allem die Tortengrafik, die die globalen Marktanteile der verschiedenen biometrischen Technologien zeigt. Je nach Kontext unterstreichen die Autorinnen dementsprechend, dass die Fingerabdrucktechnologie weiterhin die führende bleibt und eine andere – im og. Fall die Venenerkennung – absehbar größere Anteile des Weltmarktes erobern wird (etwa 10 % bis 2014).

Sicherheit bedeutet Wachstum. So absurd es sein mag, dass Sicherheitstechnik gar nicht wirklich sicher ist, sondern sehr fehleranfällig, ist doch genau dieser Umstand eines ihrer basalen und sie als marktwirtschaftlich taugliches Produkt auszeichnenden Merkmale. Zwar wird im Kontext der medialen Aufmerksamkeit rund um biometrische Systeme deren „Verwundbarkeit" ein zentraler Interventionspunkt, an dem einer ihrer zentralen Zwecke – die Erhöhung der Sicherheit von Authentifizierungsprozessen – in Frage gestellt wird. Gleichzeitig bedeutet genau dieser Umstand Entwicklungspotential. Eng verknüpft mit dem Diskurs um den wachsenden Markt für biometrische Innovationen ist der um die, dank eines immer besseren Verständnisses der technischen Anforderungen biometrischer Anwendungen, stets raffinierter werdenden Implementationen. Die Fehler der Technik sind ihr Wachstumsmotor. Sie sind Herausforderungen für ihre weitere Verfeinerung. Ein typisches Äußerungsmuster ist hierbei zum Beispiel:

---

[513] Maltoni u. a. 2009, S. 54.

[514] Ohne genauere Quellenangabe greifen verschiedene Wissenschaftlerinnen auf diese Daten zurück, vgl. bspw. ebd., S. 12 oder Kwon 2009, S. 7 f. oder Xueyan und Shuxu 2008, S. 537.

[515] Vgl. Thieme 2009. Dieser Marktbericht ist bei weitem nicht der einzige dieser Art. Für derartige Marktstudien zur Biometrie gibt es wiederum einen eigenen Markt.

> „These advantages have led to the development of a wide variety of fingerprint sensor concepts and designs, driven by a growing understanding of the challenges involved in reliable fingerprint sensing."[516]

Des Weiteren ist gerade auch der Schutz gegen Überwindungsfehler eine niemals endende Quelle für technische Weiterentwicklung. Im »Handbook of Biometric Anti-Spoofing« heißt es:

> „[…] it is safe to say that spoofing is still in its early stages of existence, and it has a huge potential to bear new challenges due to a large number of biometrics traits and a growing range of available sensors. […] Spoofing techniques are fast becoming more sophisticated and anti-spoofing measures have only a limited validity period, indicating that ongoing efforts from both industry and academia is needed."[517]

Es ist klar, dass in diesem Rahmen den bisherigen Entwicklungen immernoch – ganz im Sinne der inzwischen allgemein beliebten Software-Versionierung von Marktprogrammen (Web 2.0, Industrie 4.0 o. ä.) – eine noch neuere Entwicklung im gleichen Fahrwasser folgen muss. Exemplarisch ist hier das FBI-Projekt mit dem Namen *Next Generation Identification* (NGI) zu nennen.[518] Hiermit wird insbesondere die multimodale Biometrie forciert und sukzessive das IAFIS des FBI um z. B. Gesichts- Iris- oder Handabdruckdatenbanken ergänzt.

4.4.3 Institutionalisiertes Misstrauen

Herbert Burkert erwähnt in seinem Aufsatz über *Privacy-Enhancing Technologies* (PET) die bedeutende Rolle des Vertrauens. Vertrauen könne sogar die Antwort auf das Überwachungsparadox sein, dass Überwachung wiederum durch Überwachung überwacht werden müsse usw.[519] In der heutigen Überwachungsgesellschaft sei es nicht lediglich ein Zeichen von Naivität, dass Menschen weiterhin die kommunikativen Möglichkeiten des Internets nutzen, sondern mit Burkert auch ein Zeichen für die erhebliche soziale Bedeutung von Vertrauen:

---

[516] Setlak 2004, S. 30

[517] Erdoğmuş und Marcel 2014, S. 10.

[518] Siehe hierzu: https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi, letzter Abruf: 29.7.2017. Die Erweiterung des *Integrated Automated Fingerprint Identification System* (IAFIS) des FBI begann 2008 (vgl. Jain, Feng und Nandakumar 2010, S. 37). Siehe Pender 2010 für einen Überblick zur Projektplanung. Die Bürgerrechtsorganisationen *Electronic Frontier Foundation* (EFF) und *Electronic Privacy Information Center* (EPIC) kritisieren NGI und stellen viele Hintergrundinformationen bereit (siehe https://www.eff.org/foia/fbis-next-generation-identification-biometrics-database sowie https://epic.org/privacy/fbi/ngi.html, beide letzter Abruf: 4.8.2017).

[519] Vgl. Burkert 1997, S. 139.

> „Trust as a social phenomenon [...] involves a conscious decision to interact *although* there is risk. Relationships in which risk taking is eliminated or essentially reduced by devices, whether of a technical or a social nature, leave little room to display trust. They also provide few opportunities to be trusted and thus feel appreciated, needed, and involved. The less these feelings occur the looser the bonds that hold a society together may become. [...] The capability of people to insert into these [surveillance] systems acts of conscious risk taking in social relationships (i.e., trust) ensures the functioning of society in spite of these mechanisms."[520]

Allerdings müsse genau dies auch im Design von PETs etwa dadurch berücksichtigt werden, dass Menschen ihre Identität bewusst und selektiv anderen offenlegen könnten. Irma van der Ploeg bezieht sich auf Burkert im Rahmen ihrer Kritik an PET, die in zirkulärer Weise die Probleme mit derselben Technik lösen wolle, die diese Probleme erst erzeuge. Eine *Privacy*, die eigentlich Heimlichkeit meint, würde eher einer „Institutionalisierung des Misstrauens" dienen.[521]

Die Kritik geht einher mit der Analyse, dass die Praktiken der Überwachung und die Idee individueller Moral oder des Rechts auf Privatsphäre Teil derselben historischen Entwicklung sind.[522] Die Sammlung von Informationen und die systematische Überwachung sind Teile des modernen Staats, in dem Verwaltungs- und Registrierungspraktiken großer Massen von Informationen die Staatsbürgerin als Datenkonglomerat überhaupt erst entstehen lassen. Eine Identifizierbarkeit von Individuen aufgrund miteinander verknüpfbarer Bevölkerungs- oder persönlicher Daten impliziert gleichermaßen die Idee, „that the identity of the individual person is naturally given, static and knowable".[523] Das Personenkonzept der Biometrie ist ebenso mechanistisch-essentialistisch. Demnach gibt es mess-, objektivierbare und nicht willentlich veränderliche körpergebundene Eigenschaften, die ein Individuum unentrinnbar an eine von ihm nicht beeinflussbare Identität binden, die in ihrer Auslegung eine soziale ist – allerdings eine, die von außen vorgenommen wird. Die mit der „registrierten Identität" zugeschriebene ist eine, die potentiell keinen Zugang zu einer bestimmten Ressource hat oder die potentiell kriminell ist oder genau andersherum. Sie ist definiert über eine soziale Abgrenzung, die nicht allein auf Basis einer gleichberechtigten Aushandlung abzusichern ist.

Es ist eine wichtige diskurspolitische Entscheidung, in Bezug auf biometrische Technologien nicht von Sicherheits-, sondern von Kontroll- oder Überwachungstechnologien zu sprechen, auch wenn beides – ähnlich wie die PET – lediglich verschiedene Ausprägungen ein und desselben Problems sind. Als identitätspolitische Regelungsinstrumente reagieren sie auf die vermeintlich stets wachsende Unsicherheit des Iden-

---

[520] Ebd., S. 139 f.

[521] Bei Ploeg heißt es: „institutionalize *dis*trust", Ploeg 2005, S. 33, Hervorhebung im Original.

[522] Vgl. ebd. Siehe hierzu auch Lyon 1994.

[523] Ploeg 2005, S. 27.

titätsbetrugs und sind Teil des Versuchs – ähnlich wie Register, Pässe, Sozialversicherungsnummern – eine verlässliche und verbindliche Zuordnung von Individuen zu Organisationen, Staaten oder Eigentum vorzunehmen, also Sicherheit herzustellen. Sie bergen andererseits selbst derart viele Unsicherheiten, dass sie auf anderer Ebene das Sicherheitspositiv konterkarieren und die gleichen Probleme, zu deren Bekämpfung sie konstruiert sind, neu erzeugen oder gar verstärken. Mehr Kontrolle und Regelung wird notwendig. Zudem greift die Präventivlogik auf panoptischer Ebene: Die Systeme könnten funktionieren, also verhalten wir uns anders, schränken uns in Bedürfnissen ein. Der Begriff Kontrolltechnologie oder noch besser sogar Überwachungstechnologie bezieht die problematischen Aspekte und die Konsequenzen der Biometrie demzufolge wesentlich weniger euphemistisch und treffender ein.

5 Didaktische Aufbereitung – Fingerabdruckerkennung im Kontext

Ein bedeutender Teil der Forschungsarbeit war der Versuch, das gewählte Thema didaktisch sinnvoll aufzubereiten, um erprobte Lehr- und Lernmaterialien für eine kritische und emanzipatorische Annäherung an die gesellschaftlichen Probleme und Fehler einer vielbeworbenen Überwachungstechnologie aus informatischer Perspektive entwickeln zu können. Planung, Durchführung und gesammelte Erfahrungen sind hierbei Teil dieses vorletzten Kapitels.

In den Aufbau der allgemeinen und vor allem der detaillierten Konzeptionierung des durchgeführten Workshops, der Unterrichtsreihe und des Seminars, die im Folgenden vorgestellt werden, sind verschiedene Planungselemente eingeflossen. Dazu gehören einerseits didaktische Leitfäden[524] und Anregungen aus verschiedenen Unterrichtskonzepten.[525] Andererseits zählen vor allem aber Erfahrungen aus der eigenen Lehre, insbesondere der Informatikdidaktikausbildung in Verbindung mit zahlreichen Hospitationen und intensiver Auseinandersetzung über Planung des Informatikunterrichts in verschiedenen Schulstufen zusammen mit den vielen Lehramtskandidatinnen dazu. Besonders inspiriert haben mich allerdings die verschiedenen Entwürfe von Projektunterricht/Unterrichtseinheiten, die im Rahmen des Unterrichtskonzepts »Informatik im Kontext«[526] entstanden sind.

In vier Schritten wird die Erarbeitung der Eckpunkte eines interdisziplinären Lern- und Lehrkonzepts zur Fingerabdruckerkennung in diesem Kapitel dargestellt: Der didaktiktheoretische Hintergrund wird im Kapitel *Zugrundeliegende didaktische Ansätze* (5.1) eingeführt. Das für die selbst durchgeführten Lehrveranstaltungen entwickelte Konzept wird im Kapitel *Konzeption eines Lehr- und Lernprojekts zur Fingerab-*

---

[524] Vgl. Meyer 2014 für allgemeine Unterrichtsplanung und für spezifisch informatikdidaktische Entwürfe vor allem Hartmann, Näf und Reichert 2007 sowie Schubert und Schwill 2011.

[525] Konkrete Beispiele für Stundenentwürfe für den Schulunterricht anderer Fächer von Lehramtsabsolventinnen gibt es beispielsweise auf den persönlichen Seiten des Schulpädagogik-Professors Hilbert Meyer: http://www.staff.uni-oldenburg.de/hilbert.meyer/28601.html, letzter Abruf: 29.7.2017; für Informatik auf dem Berlin-Brandenburger Bildungsserver: http://bildungsserver.berlin-brandenburg.de/schule/lehrerinnen-und-lehrer/lehramtsanwaerterinnen/informatik-lehramt/lehramt-inf-lehrproben/?L=O%27A%3D0, letzter Abruf: 29.7.2017.

[526] Siehe hierzu bereits die Ausführungen im *Kapitel 1.3 Vorgehen* (S. 19) sowie gleich im *Unterkapitel 5.1.1 Die Diskursanalyse als Teil des didaktisch-methodischen Konzepts* (S. 174). Ein schönes Beispiel für ein sicher nicht nur im schulischen Kontext einsetzbares Lehr- und Lernprojekt ist die Reihe von Gramm, M. Hornung und Witten 2011, in der ein Bausteinkonzept aus einzelnen Lernabschnitten, die über verschiedene Lernpfade unterschiedlich durchgeführt werden können, große Flexibilität in der konkreten Umsetzung der Lerneinheit bietet.

druckerkennung (5.2) erläutert. Im anschließenden Teil, *Umgesetzte Lehr- und Lernprojekte* (5.3), wird über die durchgeführten Projekte berichtet sowie die dafür und danach angepassten Konzepte vorgestellt. Schließlich werden wesentliche Erkenntnisse der Umsetzung des Konzepts und Anpassungsvorschläge im Schlussteil zusammengefasst.

5.1 Zugrundeliegende didaktische Ansätze

5.1.1 Die Diskursanalyse als Teil des didaktisch-methodischen Konzepts

»Informatik im Kontext« nimmt unter anderem den Begriff einer informatischen Allgemeinbildung mit auf, wie Jochen Koubek ihn formuliert hat:

> Diese „ist gekennzeichnet durch Wissen und Erfahrung um gesellschaftliche Bedeutung, Möglichkeiten und Grenzen von IKT, Chancen und Risiken der Informationsgesellschaft. […] Sie behandelt das uns alle Angehende und richtet sich an alle. Eine solche informatische Bildung ist […] Allgemeinbildung."[527]

Zu ihr gehören sowohl die soziokulturelle als auch die technische Dimension. Für beide formuliert Koubek bestimmte Niveaus an Kompetenzen, diskursanalytische wie technische, die miteinander verzahnt im Rahmen einer solchen informatischen Allgemeinbildung erworben würden.[528] Beginnend mit der Fähigkeit, die „Wirkungen von Informationstechnik in der eigenen Lebenswelt [zu] erkennen", daran anknüpfend diese „Wirkungen zu Themen [zu] strukturieren", darüber hinaus „[w]eitere Probleme dieser Themen [zu] kennen", die „Grundbegriffe [zu] verstehen, mit denen diese Themen in verschiedenen Quellen beschrieben werden" bis schließlich dahingehend, das „Fachvokabular in Diskussionen und Referaten aktiv [zu] verwenden", werden die zu erlernenden diskursanalytischen Kompetenzen beschrieben.[529] Gleichzeitig hierzu sind die qualifikatorischen Stufen im technischen Bereich zu erwerben. Das beginnt damit, die „technischen Hintergründe zu Kernthemen [zu] kennen", dann die „Komponenten der Techniken [zu] kennen", weiter „Aufbau und Funktionsweise der Informatiksysteme [zu] verstehen", auf nächsthöherem Level die „Technik im Rahmen schulischer Möglichkeiten [zu] erstellen und [zu] modifizieren" und gipfelt in der Fähigkeit, „Probleme der eigenen Lebenswelt mit informatischen Methoden [zu] lösen".[530] Erst wenn in beiden Bereichen die jeweils höchsten Niveaus erreicht sind, sei es für die Lernenden möglich auf noch höherer Ebene „Zusammenhänge von IKT und Gesellschaft [zu] verstehen" und schließlich auch „Einflussmöglichkeiten und Grenzen technischer Gestal-

[527] Koubek 2005, S. 61.

[528] Vgl. ebd., S. 62 ff.

[529] Ebd., S. 62 f.

[530] Ebd., S. 64.

tung [zu] erkennen."[531] Der Begriff der Diskursanalyse ist hierbei sehr weit gefasst und impliziert nicht unbedingt, genauere kritische begriffliche Feinanalysen durchzuführen, sondern läuft eher auf eine Befähigung hinaus, fachlich kompetente Diskursteilnehmerin zu werden.

Auf universitärer Ebene hat die Arbeitsgruppe »Informatik in Bildung und Gesellschaft« am Institut für Informatik an der Humboldt-Universität mehr als zehn Jahre lang die umfangreiche Lehrveranstaltung »Informatik & Informationsgesellschaft II: Technik, Geschichte und Kontext der Informatik« von Wolfgang Coy, Jochen Koubek, Jens-Martin Loebel und Agata Królikowski erfolgreich angeboten. Sie wurde eine Zeit lang mit Organisations- und Diskursanalysen als praktischen Übungen begleitet. Ganz im Sinne eines interdisziplinären Ansatzes wurde ein politikwissenschaftliches Analyseschema von Werner Patzelt genutzt,[532] mit dem statt eines politischen Untersuchungsgegenstands, wie bspw. einer Partei, ein technischer, wie bspw. ein Biometrie-System oder eine bestimmte gesellschaftliche Debatte um eine Technologie, in den vier Dimensionen Macht, Normen, Ideologie und Kommunikation untersucht wurde.[533] Mit Hilfe dieser Kategorien lässt sich Entscheidungsgründen, Weltbildern und nicht offen liegenden oder von Vorurteilen, naiven Vorstellungen geprägten Begriffsimplikationen zentraler Akteure rund um eine Technologie, die sich wiederum in technischen Entwürfen und Umsetzungen manifestieren, auf den Grund gehen. Dabei können Fragen wie die folgenden behilflich sein:

- *Macht*: „Wer hat welche und worauf gründende Chancen, was gegen wen durchzusetzen? Wo wurde bzw. wird tatsächlich von wem gegen Widerstreben wessen was durchgesetzt, und wo werden von wem zu wessen Nachteil welche Entscheidungen verhindert?"[534] Ein besonderer Fokus könnte, bezogen auf meine Analyse, auf den *Usees* liegen.

- *Ideologie*: Welche Art von verzerrter oder selektiver Wahrnehmung der Wirklichkeit haben die Akteure? Aus welchen Gründen? Wie unterscheiden sie sich? Welche Folgen für das Handeln der Akteure haben sie und wie verändert dies wiederum die Wirklichkeit?

- *Normen*: Welche technischen, rechtlichen oder ethischen Regeln, welche Traditionen und Konventionen bestimmen das Handeln der Akteure? Welche erwarten sie, welche befolgen sie?

[531] Ebd., S. 65.

[532] Vgl. Patzelt 2007, S. 38.

[533] Vgl. Koubek und Loebel 2007, S. 10 ff.

[534] Patzelt 2007, S. 41.

- *Kommunikation*: „Wer kommuniziert mit wem auf welchen ‚Kanälen' worüber aus welchem Grund, mit welchem Zweck und mit welcher Wirkung?"[535]

Patzelt selbst beschränkt die Methode der Diskursanalyse eigentlich nur auf die Erschließung des Bereichs der Kommunikation. Gleichzeitig ist sie aber unser einziger Zugang zu den anderen drei Dimensionen. Die Art, wie einzelne Akteure kommunizieren, gibt Aufschluss über die Machtverhältnisse zwischen den Akteuren (Individuen, aber vor allem auch Organisationen) und über ihre Weltbilder. Auch Normen werden kommuniziert. Sie wiederum stabilisieren oder beschränken die Macht bestimmter Akteure. Bedeutsam ist, dass die Diskursanalyse ein Instrument ist, um Machtbeziehungen kritisch zu rekonstruieren – mit ihr lässt sich „die Frage danach [beantworten], *was zu einem bestimmten Zeitpunkt von wem wie sagbar* war bzw. sagbar ist."[536] Letztlich ist ein Analyseschema wie das von Patzelt auch höchstens ein erster Einstieg in einer Kategorisierung zu erfassender Ebenen – es kann keine detaillierte Anleitung für die eigentliche Analyse bieten.

In der konkreten Anwendung innerhalb eines Unterrichts- oder Seminarkonzepts bietet es die Möglichkeit einer Strukturierung der in der Inhaltsanalyse verschiedener Texte, aber auch Bilder, Tonmitschnitte oder Filme, herausgestellten Äußerungen über eine Technik. Bezogen auf das Thema dieser Arbeit kann ein konkretes Fingerabdruckerkennungssystem in den Blick genommen und dazu veröffentlichte Artikel entlang der oben genannten Fragekomplexe inhaltlich analysiert werden. Beispieltechniken, die von den Studierenden im durchgeführten Seminar[537] selbständig gewählt wurden, waren beispielsweise das riesige biometrische Enrolment der *Unique Identification Authority of India* (UIDAI), das Fingerabdruckbezahlsystem von Edeka oder das israelische *Basel*-Projekt zur biometrischen Grenzkontrolle von palästinensischen Angestellten.

5.1.2 Praktische Fehlererfahrung als Teil des didaktisch-methodischen Konzepts

Die diskursanalytische Annäherung an ein Informatik-System soll eine differenzierte Beurteilung der politischen, sozialen oder ökonomischen Zusammenhänge, Machtgefälle und Interessengeflechte, innerhalb derer eine Technik wie Fingerbilderkennungssysteme etabliert werden kann, ermöglichen. Ergänzt wird dieser Ansatz durch

[535] Patzelt 2007, S. 44. Die Kommunikationsanalyse ist für Patzelt einerseits „Sprachanalyse, andernteils […] Diskursanalyse, wo es – über eine Klärung der tatsächlichen Verwendung von politischer Sprache und politischen Argumentationsformen hinaus – darum geht, auf welche Weise im Diskurs die Geltung von Aussagen, Positionen und Wertvorstellungen erzeugt und außerdem von einer faktischen auch zu einer mit Vernunftgründen annehmbaren werden kann." (ebd., S. 44 f.).

[536] M. Jäger 2008, S. 386, Hervorhebung im Original.

[537] Siehe *Unterkapitel 5.3.3 Universitätsseminar am Institut für Informatik, HU Berlin, 2012/13* (S. 218).

eine praktische Analyse der Systeme mittels experimentierenden Lernens. Die Lernenden nehmen hier die Rolle kritischer Testerinnen ein, die verbalisieren und auch durch reproduzierbare Demonstration beschreiben können, welche Benutzungsprobleme auftreten oder wo Soft- und Hardware nicht vorgegebenen Erwartungen entsprechend funktionieren. Es soll ein praxisorientiertes Lernen aus Fehlern sein. Der Begriff des Fehlers soll an dieser Stelle weit gefasst werden: es geht um eine Aktivität innerhalb eines Bezugssystems, die dessen Regeln zuwiderläuft und eine Störung verursacht. Hierbei kann das Ausmaß der Störung anhand der Konsequenzen für eine Gesellschaft – beispielsweise hohe ökologische, materielle oder menschliche Kosten – und anhand ihrer Reversibilität charakterisiert werden.[538] Die pädagogische Psychologin Maria B. Spychiger beschreibt das „Lernen aus Fehlern" als ein „interaktives Geschehen", in dem die involvierte Person

> „in der Lage sein [muss], die Konsequenzen eines Fehlers als *Rückmeldung* aufzunehmen. Es ist ein Wechselspiel zwischen ihr und den in der Situation gegebenen Faktoren. Auch die Sanktionen, auf die sich eine Gesellschaft im Rahmen der Entwicklung ihres Rechtssystems geeinigt hat und die einsetzen, wenn Personen die gegebenen Normen nicht befolgen, haben die Funktion der Rückmeldung. […] Spezifischer erfolgt die wechselseitige Einflussnahme oft in der sozialen Interaktion […] In deren Folge steht idealerweise die individuelle Bereitschaft, Verantwortung für die weitere Entwicklung der Situation und des Lernprozesses zu überehmen."[539]

Die Zielkompetenz hierbei ist die Fähigkeit zum *Perspektivenwechsel*.[540]

Das Lernen aus Fehlern lässt sich gut mit dem konstruktivistischen Lehr- und Lernmodell des *erfahrungsbasierten Lernens* vereinbaren. Der Bildungstheoretiker David Kolb, der sich wiederum auf John Dewey, Kurt Lewin und Jean Piaget bezieht, beschreibt das Lernen als einen vierstufigen Prozess aus konkreter Erfahrung, reflektierender Beobachtung, Abstraktion von Begriffen und aktivem Experimentieren.[541] Ein Lernprozess kann an irgendeiner dieser Stufen einsetzen, da sie spiralförmig wieder und wieder durchlaufen werden, und zu immer neuen Erkenntnisebenen führen. Während die Diskursanalyse Reflexion und Generalisierung von Konzepten ermöglicht, können die praktischen Anteile des Lehr- und Lernkonzepts konkrete Erfahrung ermöglichen, die wiederum durch anfängliches und später mit immer mehr Wissen angereichertes Experimentieren entsteht. Der kritische Blick ist hierbei auch Teil des Experimentierens. Dieses impliziert ein durch Fehler geleitetes Lernen.

---

[538] Vgl. Spychiger 2008, S. 277. Die hier übernommene Klassifikation soll an dieser Stelle lediglich eine Orientierung bieten. Im *Kapitel 2.5 Fehlerbegriffe* (S. 72) wurde detaillierter auf verschiedene Fehlerbegriffe in den Disziplinen und speziell in der Informatik eingegangen.

[539] Ebd., S. 279.

[540] Ebd., S. 274.

[541] Vgl. Kolb 1985.

In der Informatik ist ein „fehlergetriebenes“ oder ein Trial-and-Error-Lernen sogar eine relativ intuitive Praxis vor allem im Rahmen der Software-Entwicklung. Donald E. Knuth, Verfasser des mehrbändigen Informatik-Grundlagenwerks »The Art of Computer Programming« und des Textsatzprogramms TeX, ist sowohl bekannt für die sorgsame Dokumentation seiner Programmierfehler als auch der Fehler in seinen Büchern.[542] Sein Credo, „[…] that one of the best ways to learn is by a process of trial and error“,[543] bringt ein wichtiges Selbstverständnis vieler Informatikerinnen, seien sie Akademikerinnen oder Hobbyistinnen, zum Ausdruck. Eine offene Fehlerkultur in *Software and Security Engineering* ist eine Grundlage der Entwicklung guter Software. Alltägliche *Security-Updates* in den verschiedenen laufenden IT-Systemen und die Computergeschichte zeigen, dass dies sein muss und noch ein großes Entwicklungspotential hat.

Im geplanten Lehr- und Lernprojekt sollen Fehler, die im Sinne der konstruktivistischen Didaktik einen „Motor für den subjektiven Lernfortschritt bilden“,[544] auf mehreren Ebenen aktiv reflektiert werden und so ein interessiertes, kritisch erschließendes Lernen ermöglichen: um mögliche Fehler der Systeme zu verstehen, sollen die eigenen Fehler in der Interaktion mit ihnen – zum Beispiel zu wenig Wissen darüber oder falscher Umgang damit – produktiv werden. Hierbei wird insbesondere auch die Frage nach der Relativität des Fehlers in Hinblick auf die Frage interessant, ob das System falsch konstruiert ist oder die Nutzerin es je nach ihrer Rolle dem System gegenüber (*Usee*/Administratorin/Betreiberin) falsch benutzt. Im Rahmen des didaktischen Konzepts wird die Untersuchung der Fehler biometrischer Systeme[545] in Beziehung zu den Fehlern der Lernenden gesetzt.

Zum einen erfordert dies zwangsläufig eine tiefergehende und kreative praktische Auseinandersetzung mit einem Testsystem, zum anderen eine begleitende theoretische Reflexion, das heißt, ein Erlernen von Begriffen, das Lesen von Dokumentationen und das aktive Kommunizieren mit anderen darüber. Eine grundlegende Herangehensweise ist hierbei der kritische Blick, das Lernen aus dem Finden von Fehlern, sowohl im Rahmen des eigenen Lernprozesses als auch innerhalb des Erlernten. Fehler können hierbei auf mehreren Ebenen erfahren werden: erstens als ein subjektives Scheitern zum Beispiel bei einer „falschen“ Systembenutzung oder einem „Falschverstehen“ von

[542] So veröffentlichte er die über 850 von ihm dokumentierten Fehler bei der Entwicklung von TeX zu einem stabilen System (vgl. Knuth 1989), obwohl er dies auch ein wenig als beschämend empfand (vgl. Knuth 1992, S. 28). Für einen noch nicht entdeckten Fehler – Tippfehler, logische Fehler, historische Fehler usw. – zahlt Knuth einen hexadezimalen Dollar, also 256 Cents, siehe http://www-cs-staff.stanford.edu/~knuth/books.html, letzter Abruf: 29.7.2017.

[543] Knuth 1992, S. 28.

[544] Käser 2011, S. 167.

[545] Zu den im Rahmen dieser Arbeit genutzten Fehlerkategorien genauer unter *Kapitel 2.5 Fehlerbegriffe* (S. 72).

Fachbegriffen oder Algorithmenbeschreibungen; zweitens als Wahrnehmung bereits dokumentierter Fehler wie Fehlermeldungen der Software, Angaben zur Systemperformanz oder Regeln für eine korrekte Benutzung; drittens als Entdeckung nicht offensichtlicher Funktionsfehler, Falscherkennungen, Entwurfsfehler, Dokumentationsfehler, Fehlannahmen über die Leistungsfähigkeit des Systems. Fehlererfahrungen der ersten und zweiten Ebene geben guten Aufschluss darüber, welche Missverständnisse möglicherweise immer wieder auftreten, auf welche Probleme eben auch *Usees* immer wieder stoßen können und welche dieser Probleme den Entwicklerinnen bekannt sind. Das Erfassen der einkalkulierten, aber „unsichtbaren" Systemfehler und damit das Erkennen zentraler Prinzipien der Muster*ähnlichkeits*erkennung ist Teil der dritten Ebene von Fehlererfahrungen – hier ist es beispielsweise hilfreich, existierende Algorithmen selbst zu implementieren oder in quelloffener Software Parameter so zu verändern, dass sich das Programmverhalten ändert. Hier entstehen dann Lerneffekte durch die Trial-and-Error-Methode auf Systementwurfsebene. Ähnlich kann es bei Überwindungsfehlern laufen, die ein von außen initiiertes, beabsichtigtes Fehlverhalten zur Folge haben sollen – auch hier kann die Überlistung nicht gelingen und zu einer verbesserten Strategie führen.

Durch das sukzessive informiertere „Herumprobieren" an der konkreten Implementierung eines Fingerabdruckerkennungssystems kann nun ein Begreifen einsetzen, wie es Heidi Schelhowe, ebenfalls dem konstruktivistischen Ansatz in der Tradition Deweys und Piagets folgend, in ihrem Aufsatz »Interaktionsdesign für reflexive Erfahrung« beschreibt.[546] Hierin geht es um ein „be-greifendes" Lernen mittels „Begreifbarer Technologien" oder auch „Tangibles".[547] Schelhowe beschreibt Anforderungen an die Gestaltung von Computermedien, die ein Lernen über dieses Medium selbst ermöglichen. Das heißt, dass Lernende

> „für sich selbst – ohne Instruktion – ein tieferes Verständnis entwickeln, den Ursachen selbst auf den Grund gehen können. Die Genese und die Hintergründe sind mit dem Algorithmus selbst als ausführbare und auffindbare Erklärungen implementiert und können dort aufgespürt und entdeckt werden."[548]

Be-greifen bedeutet hier also, „dass das Verstehen nicht über Instruktion von außen, sondern über eigenes Greifen und Handeln gelingt."[549] Die direkte Interaktion mit dem Computermedium, in meinem Falle konkret mit einem Fingerabdruckerkennungssystem, soll das Verständnis insbesondere auch der Grenzen seiner Funktionalität sinnlich erfahrbar machen, „die Kontrolle und den Überblick zu behalten über das, was

[546] Vgl. Schelhowe 2012.

[547] Ebd., S. 266.

[548] Ebd., S. 268.

[549] Ebd., S. 253.

die Automaten tun und wo sie versagen und menschlicher Eingriff nötig ist."[550] Nun setzt dies entsprechend den Anforderungen des „Interaktionsdesign[s] für reflexive Erfahrung" ein nach didaktischen Gesichtspunkten gestaltetes Fingerabdruckerkennungssystem voraus. Da es dies bis dato nicht gibt, wird im Rahmen der konkret in dieser Arbeit durchgeführten Projekte zunächst doch auf die real genutzten Objekte zurückgegriffen.[551] Allerdings berge die Manipulation nicht direkt für den Lernkontext entworfener *Tangibles* die Gefahr, dass die für das Lernen notwendige „kognitive Dissonanz, [das] Zurücktreten zum Zweck des Reflektierens" eher behindert werden.[552] Während gerade in Verbindung mit der Diskursanalyse die Untersuchung real im Einsatz befindlicher Geräte für oben aufgezählte Fragestellungen interessant ist, sind sie für das Verstehen von Bild- und Mustererkennungsalgorithmen allein ungeeignet, da sie diesbezüglich nahezu intransparent arbeiten. Hier wird auf klassisches in Texten oder Bildern vorhandenes Lehrmaterial zurückgegriffen.[553] Nichtsdestotrotz lassen sich aus der Arbeit mit den für die Lernprojekte genutzten kommerziellen Fingerabdruckscannern Anforderungskriterien für ein Design eines solchen Lern-Fingerbilderkennungssystems herausarbeiten, die daraus ein *Tangible* machen könnten. Das heißt, dass sie sowohl zum Verstehen-Wollen der Funktionalitätsprinzipien der Mustererkennung animieren als auch die abstrakten Konzepte, die dahinterstehen, erschließbar machen sollen. Diese „können ‚visible' gemacht werden, indem das Interface den Blick auf die inneren Vorgänge freilegt und die Prozesse in diesem Sinne transparent werden."[554]

Das schließt im konkret avisierten Lehr- und Lernprojekt mit ein, dass die Fehler nicht nur als Brüche im Sinne von Winograd/Flores erfahrbar,[555] sondern ebenfalls auf mehreren Ebenen sichtbar werden. Die Diskursanalyse nähert sich auf der Ebene der Text- oder Filmanalyse dem an, was wie über Fehler gesagt wird. Die konkrete Untersuchung des vergegenständlichten Fingerabdrucksystems wird aufzeigen, wieviele Fehler – sowohl von den systeminhärenten als auch von den Softwarefehlern, aber auch von den künstlichen Barrieren für unpassende Körper – in einer Be-greifbaren Technologie sichtbar gemacht werden können.

---

[550] Schelhowe 2012, S. 269.

[551] In den konkreten Projekten erhoffe ich mir, dies mit der entsprechenden didaktischen Begleitung, die impliziert, dass es auch um die Erforschung der Grenzen der Auseinandersetzung mit den gegebenen Objekten geht, etwas abfedern zu können.

[552] Ebd., S. 268.

[553] Siehe hierzu auch *Kapitel 3.7 Bildungsprojekte zur Biometrie und die Rolle der Fehler* (S. 124).

[554] Ebd., S. 268.

[555] Vgl. Winograd und Flores 1992.

5.2 Konzeption eines Lehr- und Lernprojekts zur Fingerabdruckerkennung

Die zentrale Idee hinter dem in diesem Kapitel vorgestellten Lehr- und Lernkonzept ist, sich ein umfassendes kritisches Verständnis über die gesellschaftliche Rolle und den Sinn einer Kontroll- und Überwachungstechnologie, wie es Fingerabdruckerkennungssysteme sind, sowohl auf technischer als auch auf sozialer Ebene verschaffen zu können. Zwischen den verschiedenen Anforderungen durch Umwelt und Akteure und den Versprechen eines idealisierten Produkts zur Fingerbilderkennung entstehen Widersprüche, die im real implementierten Informatiksystem schließlich dynamisch integriert werden – dynamisch bedeutet, dass es nie fertig ist, sondern Updates, Reparaturen und Störungen unterliegt, die auch sozial verhandelt werden müssen. Das resultierende komplexe Systemdesign soll auf verschiedenen Ebenen vor allem über seine Brüche erschlossen werden. Es ist eine induktive Herangehensweise, durch Analyse der Fehler bereits umgesetzter Systeme den Kompromiss, den sie darstellen, zu verstehen und sie entsprechend kritisch zu beurteilen.

Ganz konkret ist das Ziel, durch partielle Systemdekonstruktion zum einen zu erschließen, wie die Technik konkret funktioniert und umgesetzt ist. Zum anderen soll parallel durch Analyse medialer Debatten und verschiedener Fachveröffentlichungen über in der Praxis eingesetzte Systeme verstanden werden, worin deren sozialer Zweck besteht, unter welchen Akteurskonstellationen, mit welchen Interessen, Machtoptionen und Anforderungen sie entwickelt wurden, aus welchen historischen Entwicklungen sie entstanden sind sowie warum und in welcher Weise sie nicht wie gewünscht funktionieren. Ein besonderes Augenmerk liegt auf der Prüfung der Frage, mit welchen Auswirkungen auf ohnmächtige Akteure sie praktisch umgesetzt sind.

5.2.1 Motivation

Die Erfassung von Fingerabdrücken und Passbildern als biometrische Daten auf RFID-Chips in Reisepässen oder in großen Datenbanken ist inzwischen weltweit eine normale Prozedur geworden. Auch in geschäftlichen oder privaten Kontexten werden digitale Muster verschiedener Körpermerkmale vielfältig genutzt. In Europa hat die Nutzung biometrischer Daten ihre längste Tradition in der Kriminaltechnik. In kaum einem Kriminalroman oder -film fehlen Fingerabdrücke zur Suche nach der Täterin. Inzwischen geschieht diese natürlich mit Hilfe der sogenannten Automatisierten Fingerabdruck-Identifizierungssysteme (AFIS).

In biometrischen Systemen ist es nicht oder nur sehr eingeschränkt möglich, von außen nachzuvollziehen, wie und wie korrekt sie funktionieren. Letztlich weiß nur die Betroffene und Leute, die sie kennen, ob ein solches System sie richtig erkannt hat oder nicht. Aber wem lässt sich unter welchen Umständen einfacher vertrauen? Was heißt eigentlich dieses Kennen oder Erkennen? Nicht zuletzt diesen schwierigen Fragen soll

sich die Unterrichtsreihe spielerisch, entdeckend und kontrovers annähern. Angst und falscher Respekt vor vermeintlich perfekten Kontrollsystemen sollen abgebaut werden. Dazu soll analysiert werden, wie ein solches System modelliert und konkret implementiert ist, welche Aspekte der Signalverarbeitung und der Mustererkennung eine wichtige Rolle spielen und welche Fehler sich technisch zwangsläufig immer ergeben und inwiefern die Person, die das System nutzen muss, überhaupt davon erfährt. Außerdem soll klarer werden, dass biometrische Systeme Teil von aus bestimmten Gründen in soziale und historische Kontexte eingebetteten Überwachungstechnologien sind, die nie losgelöst von bestimmten Grundannahmen über menschliche Identität und Interessen vieler verschiedener Akteure aus Staat oder Privatwirtschaft sind.

5.2.2 Zielsetzung und Zielgruppe, didaktischer Hintergrund

Das modular angelegte Lehr- und Lernkonzept mit dem Titel »Überwachungstechnologie begreifen: Wa(h)re Identität und der Fingerabdruck« hat zum Ziel, ein kritisches Verstehen der Funktionalität und Fehler einer Kontrolltechnologie wie einem biometrischen Fingerabdruckidentifizierungssystem zu ermöglichen. Die Lernbausteine werden an den Konzepten der Initiative »Informatik im Kontext« (IniK) orientiert und für die projektorientierte Arbeit in der Schule oder der außerschulischen Bildungsarbeit für Menschen ab einem Alter von 14 Jahren entworfen, sollen aber für universitäre Seminare oder die Erwachsenenbildung im Allgemeinen erweitert werden können.

Das didaktische Konzept ist von einer starken Lebensweltorientierung im Sinne des IniK-Ansatzes[556] und im Sinne konstruktivistischer Didaktik geprägt. Das schließt ein handlungs- und praxisorientiertes Lernen ein, in dem zugleich kritisch-hinterfragendes Denken trainiert werden soll. Ganz wörtlich wird dabei auf ein *Lernen durch und an Fehler(n)* zurückgegriffen, indem die Fehler eines biometrischen Fingerabdruckerkennungssystems in den Vordergrund gestellt werden.

5.2.3 Kompetenzerwerb

Den 2008 und 2016 veröffentlichten Bildungsstandards der Gesellschaft für Informatik e.V. für die Schulinformatik[557] liegt ein langjährig entwickeltes Kompetenzmodell zugrunde, das ein breites Spektrum an auszubildenden oder weiterzuentwickelnden Fähigkeiten beschreibt, die es Schülerinnen ermöglichen soll,

> „ihr Leben in einer Informationsgesellschaft selbstbestimmt zu führen und zu gestalten. Sie nutzen dabei informatische Konzepte, um Elemente ihrer Erfahrungswelt zu verstehen, d. h. zu ordnen, zu erklären, zu gestalten und gegebenenfalls zu beeinflussen. Das Verständnis für eine informatische Sicht der Welt erschließt sich für Schü-

[556] Siehe die diesbezüglichen Erläuterungen im *Kapitel 1.3 Vorgehen* (S. 19).

[557] Brinda u. a. 2008 bzw. Röhner u. a. 2016.

> lerinnen und Schüler dabei nicht nur aus der alltäglichen Erfahrung mit digitalen Medien, zumal sich diese fortwährend rasch ändern oder erweitern, sondern erfordert einen Perspektivenwechsel von der Lebenswelt hin zu fachlich fundierter, wissenschaftspropädeutischer Auseinandersetzung."[558]

Die in dieser Arbeit entwickelten Lernmodule belangen die im Kompetenzmodell festgelegten Inhaltsbereiche *Informatiksysteme* – hier: Fingerabdruckerkennungssysteme – und *Informatik, Mensch und Gesellschaft* – hier entlang der Fragestellung, welche Risiken mit den vielschichtigen Fehlern des Biometrie-Systems verbunden sind, welche normativen, rechtlichen, ethischen und sozialen Ursachen wie Folgen dies hat und wie sich hieraus ein konkreter verantwortungsvoller Umgang damit gestalten sollte. Die Form der Auseinandersetzung mit diesen Themenbereichen soll die in den Bildungsstandards benannten Prozesskompetenzen schulen. Dazu gehören *Begründen und Bewerten*, *Darstellen und Interpretieren*, *Kommunizieren und Kooperieren*, *Strukturieren und Vernetzen* sowie *Modellieren und Implementieren*. Welche Aspekte davon in dem hier entwickelten Bildungskonzept wie berührt werden, soll kurz genauer ausgeführt werden:

- *Begründen und Bewerten /Darstellen und Interpretieren /Kommunizieren und Kooperieren* – Die kritische Beurteilung der *Wechselwirkungen zwischen Informatiksystemen, Mensch und Gesellschaft* soll in dieser Reihe das zentrale Gewicht haben. Das folgerichtige und transparente Argumentieren unter Einbezug des Fachwissens wird vor allem unter Einübung diskursanalytischer Praktiken trainiert. Dazu gehört auf der Ebene der *Reproduktion*, Argumentationen in Special-Interest-Medien (Computer-Fachpublikationen online wie offline), aber auch (auf höherem Niveau) wissenschaftlichen Fachtexten sowie netzpolitischen oder technikbezogenen Darstellungen aus anderen Medien oder wissenschaftlichen Fachbereichen wiedergeben und einzelne Aussagen logisch zu widerlegen oder zu belegen. Auf der höheren Anforderungsebene von *Reorganisation und Transfer* bedeutet es, zwischen Einzeltexten (es können auch audio-visuelle oder bildliche Darstellungen sein) Zusammenhänge herstellen, sie in ihrer Darstellungsform vergleichen und in ihre Prämissen, Schlussfolgerungen und stützenden Fakten zerlegen und interpretieren zu können. Schließlich soll auf der höchsten Anforderungsebene *Reflexion und Problemlösung* eine eigene kritische, begründete Haltung zu den analysierten Diskursstrukturen entwickelt und möglicherweise auch bildlich/diagrammatisch (z. B. Darstellung der Akteur-Netzwerke) veranschaulicht werden. Das Informatiksystem als eigener Akteur oder „Aktant" soll möglichst einbezogen werden – es soll durchdrungen und konkret auf Komponenten und Algorithmen bezogen analysiert werden, dass es als „spezifische Zusammenstellung von Hardware-, Software- und Netzwerkkomponenten zur

[558] Röhner u. a. 2016, S. 1.

Lösung eines Anwendungsproblems“ dient und damit „nichttechnische Aspekte, die durch die Einbettung in ein soziokulturelles System relevant werden, z. B. Einbeziehung der potenziellen Nutzer in den Entwicklungsprozess [oder] die ökonomischen und ökologischen Folgen.“[559]

Die Ergebnisse der diskursanalytischen Arbeit werden *gemeinsam bewertet und kontrovers* diskutiert. Zudem knüpft sich an die Betrachtung der Fehler eines Biometriesystems nahtlos die Frage der Akzeptanz derselben an – hier können sowohl historische, aber auch aktuelle politische Debatten in ein Rollenspiel einfließen, um Konzepte von Identität und Vertrauen in ihrer Vielfältigkeit zu erschließen und die Problematik der Formalisierung und Entkontextualisierung einer maschinellen Identifikation zu verstehen.

- *Modellieren und Implementieren* – Eine praktische Annäherung an ein fertig implementiertes System stellt das Nachvollziehen von verschiedenen Performanztest- und Überwindungstestszenarien dar. Anhand eines ausgewählten Systems ist es sinnvoll, bestimmte Testfälle selbst auszuprobieren. Dies bewegt sich vor allem auf den erstgenannten beiden Anforderungsebenen:
  - *Reproduktion*: Auf dieser Anforderungsebene werden zunächst Fingerabdruckscanner, die biometrischen Charakteristika und die Software praktisch wie theoretisch erkundet. Wie finden sich zentrale Komponenten des Biometrie-Systems in den Programmpaketen und Methoden wieder? Wie funktioniert der Scanner? Was wird an der Nutzerschnittstelle gezeigt? Vorhandene Mustererkennungsmodelle werden an einer konkreten Implementierung nachvollzogen und ausprobiert.
  - *Reorganisation und Transfer*:
    1. Die manuelle mit den Informatiksystemen automatisierte Praxis des Fingerabdruckabgleichs mit Papier und Druckerschwärze wird praktisch nachvollzogen und in Beziehung zur digitalen Variante gesetzt.
    2. Es werden insbesondere in der Literatur beschriebene Überwindungstests selbst ausprobiert und vorher auf die konkreten Gegebenheiten übertragen konzipiert.
    3. In gegebenem Source-Code werden die Performanz beeinflussende Parameter manipuliert und die Auswirkungen auf die Funktionalität geprüft.
  - *Reflexion und Problemlösung*: Es ist nicht vorgesehen, Komponenten eines Fingerabdruckerkennungssystems neu oder selbst zu implementieren. Es wäre allerdings möglich, eigene Testfälle inklusive Evaluation aufzusetzen.

[559] Röhner u. a. 2016, S. 11.

- *Strukturieren und Vernetzen* – Dieser Bereich ist unmittelbar an den oben schon genauer beschriebenen Prozessbereich des *Begründens und Bewertens* geknüpft. Insbesondere die selbständige Abbildung des analysierten Technikdiskurses auf ein Akteur-Netzwerk geschieht unter Rückgriff auf „sequenzielle, hierarchische oder netzartige Strukturen“ und „verknüpf[t] informatische Inhalte mit solchen in und außerhalb der Informatik“.[560]

5.2.4 Übersicht der Lerninhalte

In der aus vier Grundbausteinen, für die jeweils zwischen vier und acht Stunden Arbeitsdauer vorgesehen sind,[561] bestehenden Lerneinheit können sich die Schülerinnen mit dem Einsatz von Rechentechnik im Bereich der Biometrie praktisch wie theoretisch auseinandersetzen. Abbildung 5.1 zeigt den grundsätzlichen modularen Gesamtentwurf, der historische, diskursanalytische und praktisch-experimentierende Ansätze kombiniert.

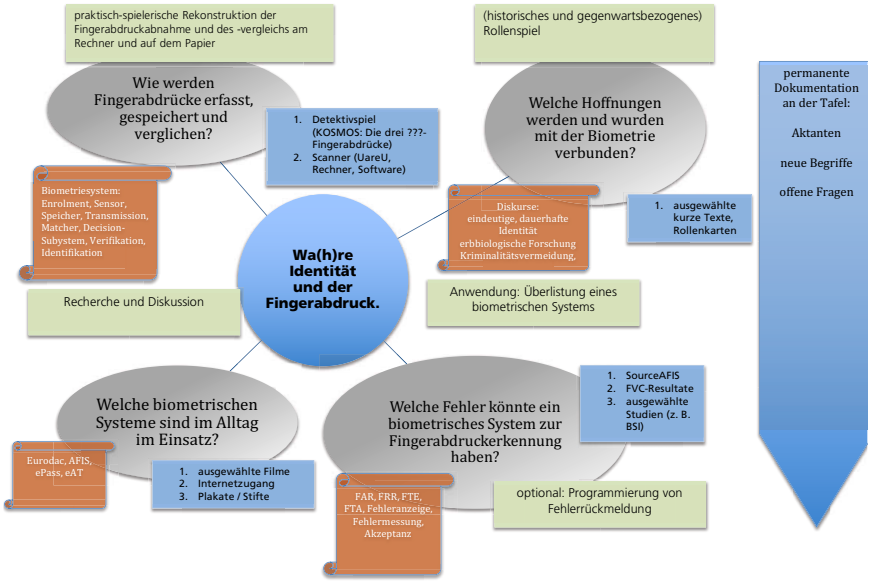


Abbildung 5.1: Die vier Grundbausteine der Lerneinheit »Überwachungstechnologie begreifen: Wa(h)re Identität und der Fingerabdruck« anhand der Leitfragen, ausgewählter Lerninhalte und -methoden.

[560] Ebd., S. 7.

[561] Das sind Mindestzeitangaben – Erweiterungen sind natürlich je nach vorhandenem Zeitrahmen konzeptuell auf jeden Fall möglich.

Auf dem Schaubild sind die Hauptfragestellungen der vier großen inhaltlichen Bausteine in grauen Ellipsen dargestellt. In den Kästen drumherum finden sich erste Hinweise für benötigtes Material, auf jeweils wichtige inhaltliche Begriffe und methodische Herangehensweisen. Die Festlegung auf konkrete Unterrichtsformen bspw. als offen, Fish-Bowl oder Gruppenpuzzle oder auf Einzel- oder Gruppenarbeit wird in den späteren Detailplanungen der Module für die jeweiligen Lehr- und Lernprojekte vorgeschlagen. Die Anordnung der Bausteine ist im Grunde flexibel und könnte auch verzahnt werden. Während der gesamten Reihe sollten zentrale Begriffe, Akteure, aber auch nicht schnell zu klärende inhaltliche Nachfragen an der Tafel, auf Plakaten oder in einem Wiki diskutiert werden.

Ein möglicher Vorschlag für eine Reihenfolge der Module und eine erste Abschätzung des Zeitaufwands wird in den folgenden Tabellen vorgenommen.

Tabelle 5.1: Gesamtplanung Lehr- und Lernprojekt
»Überwachungstechnologie begreifen: Wa(h)re Identität und der Fingerabdruck«

Leitfrage eines Moduls	*zeitlicher Umfang*	*grober methodischer Ansatz*	*Arbeitsmaterialien*
I. Wie werden Fingerabdrücke erfasst, gespeichert und verglichen?	4x45min	praktische Rekonstruktion alter und neuer Methoden in Zweier- bis Dreiergruppen, für den Erfahrungsaustausch u. U. Gruppenpuzzle o. Schülerpräsentation	je nach Gruppengröße (max. 20 Leute): 1 Rechner mit Fingerabdruckscanner inkl. Software pro Gruppe (max. 5x) 1 Detektivset pro Gruppe (max. 5x), Doku-Plakate und Stifte
II. Welche Hoffnungen werden und wurden mit der Biometrie verbunden?	2x45min	historisches und gegenwartsbezogenes Rollenspiel	Rollenkarten, ausgewählte Texte (Arbeitsblätter oder digitale Vorlagen)
IIIa. Welche Fehler könnte ein biometrisches System zur Fingerabdruckerkennung haben?	8x45min	Variante A: praktisches Austesten der Überwindung eines biometrischen Systems am Fingerabdruckscanner in Dreier- bis Vierergruppen Variante B: direkte Manipulation ausgewählter Konstanten im Quellcode, Erkennungstests mit verschiedenen gegebenen Abdrücken	Variante A: Holzleim, Schnellkleber, Graphitpulver, Pinsel, Digitalkamera, Drucker, bedruckbare Folien, Gläser, Rechner mit Fingerabdruckscanner-Software/ Fingerabdruckscanner Variante B: ausreichend Rechner mit Entwicklungsumgebung, Softwarepaketen (SourceAFIS z. B.), Fingerabdruckdatenbanken
optional IIIb. Welche Visualisierungen der Fehler sind am UserInterface implementiert worden, welche lassen sich implementieren?	2x45min	Programmierung von Fehlerrückmeldungen der Biometrie-Software	Developer-Kit Fingerabdrucksoftware, Tutorials, Entwicklungs- und Testumgebung
IVa. Welche technischen und sozialen Akteure sind an derzeitig aktiven biometrischen Systemen beteiligt?	2x45min	Recherche, Vorträge und Diskussion; ggf. Gruppenpuzzle	

fortgesetzt auf nächster Seite

Tabelle 5.1 – fortgesetzt von letzter Seite

Leitfrage eines Moduls	*zeitlicher Umfang*	*grober methodischer Ansatz*	*Arbeitsmaterialien*
optional IVb. Einladung eines Hersteller(s), Beamten, Betroffenen o. ä.	6x45min	(a) Vorbereitung von Interviewfragen (2h), (b) Fragen/Diskussion mit geladenem Gast (2h) (c) Auswertung (2h)	
optional IVc. Exkursion oder Einladung eines Hersteller(s), Beamten, Betroffenen, o. ä.	12x45min	(a) Vorbereitung von Interviewfragen (2h), (b) Exkursion (8h), (c) Auswertung (2h)	

Tabelle 5.2: Mögliche Zeiteinteilung Lehr- und Lernprojekt »Überwachungstechnologie begreifen: Wa(h)re Identität und der Fingerabdruck«

Umfang	*Stundenverteilung*
Gesamtdauer Lerneinheit ohne optionale Teile:	16 x 45 min (2-3 volle Workshop-Tage, 8 Schul-/Seminarwochen à 2 SWS oder 4 Schul-/Seminarwochen à 4 SWS)
Gesamtdauer Lerneinheit mit optionalem Teil IIIb:	20 x 45 min (3 volle Workshop-Tage, 10 Schul-/Seminarwochen à 2 SWS oder 5 Schul-/Seminarwochen à 4 SWS)
Gesamtdauer Lerneinheit mit optionalem Teil IVb:	22 x 45 min (5 volle Workshop-Tage inkl. Exkursionstag, 11 Schul-/Seminarwochen à 2 SWS oder 5,5 Schul-/Seminarwochen à 4 SWS)
Gesamtdauer Lerneinheit mit optionalem Teil IVc:	28 x 45 min (5 volle Workshop-Tage inkl. Exkursionstag, 14 Schul-/Seminarwochen à 2 SWS, davon 4 für Exkursionstag zusammenlegen oder 7 Schul-/Seminarwochen à 4 SWS, davon 2 für Exkursionstag)

5.3 Umgesetzte Lehr- und Lernprojekte

Die im vorangegangenen Kapitel vorgestellte Konzeptionierung wurde in drei verschiedenen Kontexten ausprobiert und verbessert:

1. zweieinhalbtägiger Workshop (2 Tage à 3 x 90 min, 1 Tag à 2 x 90 min) auf der „informatica feminale – 15. Sommerstudium 2012“ an der Universität Bremen vom 27. bis 29. August 2012,

2. fünfwöchige Unterrichtseinheit (10 Stunden à 90 min) am Oberstufenzentrum Handel in Berlin, in einer 11. Klasse, Leistungskurs Wirtschaftsinformatik vom 29. Oktober bis 28. November 2012,

3. ein Semester Hauptstudiums-/Master-Seminar (16 Stunden à 90 min) in der Arbeitsgruppe »Informatik in Bildung und Gesellschaft« am Institut für Informatik der Humboldt-Universität zu Berlin im Wintersemester 2012/13.

Die grobe Planung wurde für die jeweiligen Kontexte detailliert angepasst. Eine systematische, quantitative Evaluation per Fragebogen fand nicht statt – diese ist leider ein offenes Vorhaben geblieben. Auswertungen liefen weitestgehend in direkten Gruppen- oder Einzelgesprächen mit Teilnehmenden und im Falle der Schule auch

mit dem betreuenden Lehrer und sind von mir meist nachträglich protokolliert worden. Dementsprechend sind die hier erläuterten Feedbacks durch meine persönliche Bewertung gefiltert. Gesicherte Arbeitsergebnisse in Form von Protokollen, Plakaten, Essays, Vortragsfolien und Klausuren spiegeln wider, was gelernt wurde, und ermöglichen mir einen Abgleich mit den Zielen des Kompetenzerwerbs.

5.3.1 Projekt auf der Informatica Feminale, Bremen, 2012

Die Informatica Feminale ist eine seit 1998 stattfindende, zweiwöchige Sommeruniversität an der Universität Bremen. Sie richtet sich an weibliche Wissenschaftlerinnen, Praktikerinnen und Studentinnen, die entweder als Dozentinnen oder Teilnehmerinnen verschiedene Kurse zu Grundlagen der Informatik, Robotik, Softwareentwicklung, Datenbanksystemen, Mobile Net und Internet, interdisziplinären Themen mit Informatikanbindung sowie sozialen und methodischen Kompetenzen für Studium und Beruf anbieten oder besuchen können. Die Sommeruniversität soll „neuartige Maßnahmen zur Frauengleichstellung im Wissenschaftsbereich [...] entwickeln und [...] erproben."[562] Hierfür sollen „Frauen IN der Informatik aktivier[t werden], für sich und für andere Informatikerinnen ebenso wie für am Fach interessierte Frauen Orte des Austausches zu gestalten."[563] Ebenso ist die Informatica Feminale „ein Ort des Experimentierens, um neue Impulse in das Informatikstudium zu bringen."[564]

Die Veranstaltung bietet also auch einen Rahmen für Frauen, eigene Lehrkonzepte auszuprobieren. Daher habe ich mich mit einer Kurzbeschreibung für einen einwöchigen Workshop »Überwachungstechnologie praktisch verstehen am Beispiel der Fingerabdruckerkennung« beworben. Bei der Bewerbung habe ich explizit angemerkt, dass ich den Workshop als Probelauf einer Konzeption für eine an Schulen einsetzbare Unterrichtsreihe ausprobieren und mit den Teilnehmerinnen entwickeln möchte.

Die Einreichung wurde akzeptiert. Auf die Ankündigung hin (siehe unten) meldeten sich nur zwei Teilnehmerinnen an. Aber ich durfte den Workshop wegen seiner inhaltlich interessanten und ambitionierten Ausrichtung, die ein Anliegen des Sommerstudiums, neue Impulse für das Studium zu entwickeln, aufnahm, dennoch durchführen.

Ankündigung

Die biometrische Erfassung von Personen anhand eines Fingerabdrucks ist vor allem im Reiseverkehr eine Alltagskontrolltechnologie. Wie funktioniert ein solches System und warum wird ihm solch große Bedeutung als effiziente Sicherheitstechnologie beigemessen?

---

[562] https://www.informatica-feminale.de/Konzept/index.php, letzter Abruf: 29.7.2017.

[563] Ebd.

[564] Ebd.

Wir testen gemeinsam ein *Open-Source-Automated-Fingerprint-Identification-System*. Dazu setzen wir uns zum einen mit den Prämissen und Folgen biometrischer Anwendungen in alltäglichen Kontexten auseinander. Zum anderen vollziehen wir den Systementwurf und die konkrete Umsetzung im Quellcode nach, (re-)implementieren einzelne Aspekte selbst. Der Schwerpunkt liegt auf dem kritischen Systemtest, der sowohl die statistisch messbaren, einkalkulierten Fehler als auch die Einbettung bestimmter sozialer Diskurse und Kontrollparadigmen in technische Systeme transparent zu machen sucht. Wir trainieren so das Verständnis klassischer, aber auch agiler, partizipativer Softwareentwicklungsprozesse, der Technikfolgenabschätzung und die Auseinandersetzung mit technischen Standards.

Lernziele

1. Die Teilnehmerinnen können die grundlegende Funktionalität und Bestandteile eines biometrischen Systems beschreiben.

2. Die Teilnehmerinnen können die Elemente eines generischen Biometrie-Systems in real existierenden Verifikations- und Identifikationssystemen (Eurodac, Meldestelle, Zugangskontrolle) wiedererkennen.

3. Die Teilnehmerinnen können wichtige Parameter der Performanzmessung eines Fingerabdruckerkennungssystems benennen und praktisch einordnen.

4. Die Teilnehmerinnen können selbständige Recherchen zu den Akteuren rund um ein real existierendes Fingerabdruckerkennungssystem durchführen und diese systematisieren.

5. Die Teilnehmerinnen können ein Low-Budget-Fingerabdruckverifikationssystem überlisten.

6. Die Teilnehmerinnen setzen sich intensiv mit kommunikativen und kontextuellen Aspekten einer Identität und eines menschlichen Einander-Erkennens auseinander und Diskutieren die soziale Rolle der Begriffe.

Voraussetzungen

Erwartet waren maximal zehn Teilnehmerinnen (Studentinnen, Absolventinnen und in der IT-Branche tätige Frauen), bei denen ein gewisses technisches Bastelbedürfnis gekoppelt mit einem Interesse an sozialer Einbettung von Technik vorausgesetzt wurde. Die Fähigkeit zur Bedienung und Nutzung einer Entwicklungsumgebung wie Eclipse bzw. das verstehende Lesen von Quellcode in Java oder C# und Grundkenntnisse in der objektorientierten Programmierung waren als hilfreich angegeben.

Real teilgenommen haben zwei fertig ausgebildete Informatikerinnen, eine als Linux-Systemadministratorin beruflich tätig, die andere Java-Entwicklerin/wissenschaftliche Mitarbeiterin. Das informatische Vorwissen war also auf einem sehr hohen Niveau.
Folgende Materialien und Ausstattung waren nötig und in der Universität vorhanden:

- Software: SourceAFIS, Adobe Photoshop oder Gimp; nötiges Betriebssystem: mindestens MS Windows XP oder anderes mit aktueller Java VM,
- Hardware:
  - möglichst für jede Teilnehmerin einen aktuellen Rechner (nur wenn kein eigener Laptop vorhanden) in einem LAN oder mit WLAN-Zugang,
  - Beamer oder Smartboard, Whiteboard oder Tafel,
- Räumliche Anordnung der Arbeitsplätze: am 1. Tag kleiner, relativ dunkler Seminarraum mit etwa 15 Plätzen, 2. Tag heller großer Raum, Einzeltische zu einer großen Arbeitsfläche zusammengeschoben,
- Lehrmaterialien: eine große klappbare Tafel, ein Flipchart, diverse Eddings, Kopierpapier, Schere.

Für folgende Materialien sorgte ich selbst:

- handelsüblicher *DigitalPersona U.are.U-4000*-Fingerabdruckscanner mit optischem Sensor für den Alltagseinsatz,
- für die Fake-Finger-Tests (orientiert an den Anleitungen von Kaseva/Stén):[565]
  - Variante Gelatine-Finger über Abdruckform direkt in Heißkleber:
    * Gelatine-Platten,
    * Klebepistole mit sechs Patronen und Ständer (wg. Kühlung),
  - Variante Gelatine-Finger über Form, die mit latentem Fingerabdruck als Vorlage auf Kupferplatine geätzt wird:
    * Babypuder (mit Talkum) – ungetestet,
    * Backpulver (erfolglos getestet, aber evtl. mit Ruß? - als Ersatz für Speisestärke),
    * Bleistift mit Anspitzer für Graphit (besser geeignet: Graphitpulver),

[565] Siehe Kaseva und Stén 2003a sowie die zugehörigen genaueren Beschreibungen auf der inzwischen nur noch bei *archive.org* verfügbaren Webseite http://web.archive.org/web/20131003031058/http://www.stdot.com/pub/ffs/index.html, letzter Abruf: 29.7.2017.

    * Tesa-Film (daumenbreit),
    * Malpinsel,
    * 4 Kupferplatinen, auf die die Fingerabdruckform geätzt wird,
    * Entwickler für den foto-sensitiven Layer auf der Platine (auch möglich: Platinen mit bereits fertiger Fotobeschichtung),
    * Schälchen für den Entwickler,
    * Ätznatron (NaOH),
    * Eisen(III)chlorid (FeCl3),
    * Mini-Cutter (vermutlich unnötig),
- Papierdecken als Unterlagen zur Schonung der Tische,
- reinweißes Kopierpapier,
- *nach Durchführung weiter ergänzte Liste* (folgendes musste alles noch zusätzlich während des Workshops besorgt werden):
    * Wasser (für Gelatine-Platten),
    * Wasserkocher,
    * möglichst Zugriff auf einen Kühlschrank,
    * Schüsselchen für das heiße Wasser (besser: diverse Dosierschälchen und Stäbchen),
    * Esslöffel zur sanften Dosierung des kalten Aufweichwassers für die Blättchen,
    * geeignetes Geschirr/leere Flaschen für die Abdrücke,
    * Kelle für das Aufweichen und anschließende Erhitzen der Gelatineblättchen über dem Wasserdampf des Schüsselchens,
    * Arbeitsschutzbrille,
    * Schutzhandschuhe/Einweghandschuhe,
    * sehr feiner, weicher Pinsel (bspw. aus Detektivspielen für Fingerabdruckabnahme), Makeup-Pinsel und einfache Schulmalpinsel sind zu grob,
    * Raum mit gutem Tageslicht oder mindestens eine Lampe, deren Bestrahlung flexibel einstellbar ist, für die Fotos der sichtbar gemachten Abdrücke.

- Arbeitsmaterialien zum Testen des Nachbaus von Fake-Fingern auf Basis der Beschreibungen des Chaos Computer Clubs:[566]
  - Sekundenkleber (muss Cyanoacrylate enthalten),
  - Holzleim,
  - bedruckbare Folien (Laserdrucker),
  - Lineal,
  - Strohhalm,
  - geeignete Digitalkamera, hier verwendet: NIKON Coolpix 5400 (hochauflösende Digicam mit Makro-Funktion) und
  - 64 MB SD-Speicherkarte.

Umriss des Aufbaus und der Themen – Verlaufsplanung

Zunächst war ein einwöchiger Workshop mit 28 45-minütigen Stunden auf fünf Tage verteilt angedacht, pro Tag etwa fünf bis sechs Stunden. Nachdem sich allerdings nur zwei Leute anmeldeten, wurde der Workshop auf 14 45-minütige Stunden reduziert.

Da der Workshop hier erstmalig ausprobiert werden und die Weiterentwicklung meiner ersten inhaltlichen Planungsideen ermöglichen sollte, erarbeitete ich zwar eine grobe Verlaufsplanung, die einige dieser Ideen bereits etwas detaillierter aufnahm, aber hielt mir offen, das Ganze komplett zu verändern und dies auch so zu kommunizieren.

Ein Hauptansatz war, möglichst frühzeitig ein praktisches Verstehen zu ermöglichen und daher direkt mit dem Vorführen des Systems und frühzeitig mit dessen Überlistung einzusteigen – von dort ausgehend sowie parallel dazu sollten nach und nach ein vertieftes Verständnis der Funktionsweise, des Aufbaus und der Fehler eines Fingerabdruckerkennungssystems ermöglicht werden.

Die erste Grobplanung war dementsprechend wie folgt:

[566] Siehe starbug 2004 sowie o. V. 2005.

Tabelle 5.3: Grobplanung Lehr- und Lernprojekt „Überwachungstechnologie praktisch verstehen am Beispiel der Fingerabdruckerkennung“, Informatica Feminale

Zeit	*Themenkomplex*	*Aktivitäten*	*Arbeitsmaterialien*
TAG 1 9-12.30	Fehlerdimension I: Biometrische Systeme überlisten	**bis 9.10 Uhr:** Vorstellungsrunde, Erwartungen **bis 9.30 Uhr:** Vorführung der U.are.U.-Systemanmeldung sowie Durchgehen der zugehörigen Software, inkl. Enrolment mit Aufgabe: Notieren Sie während der Vorführung auf den Karteikarten wichtige oder unbekannt erscheinende Begriffe, die fallen, und die Komponenten und Vorgänge des Fingerabdruckerkennungssystems, die Sie beobachten können. **bis 9.45 Uhr:** Zusammentragen der Begriffe an der Tafel, zusammenfassender Vortrag der Dozentin **bis 10.30 Uhr:** Textstudium mit Notizen zu folgender Aufgabe: Lesen Sie die Anleitungen, mit der Sie das System, das ich Ihnen gezeigt habe, knacken könnten und überlegen Sie sich, wieso das funktionieren könnte.	Sammelstapel mit Karteikarten für offene Begriffe, Stifte, Plakat für Erklärungsansätze für Lektüre der Anleitungen zum Fake-Finger-Nachbau: Texte von Kaseva, Stén 2003: *Fooling Fingerprint Scanners* sowie die zugehörigen Anleitungen Dies.: *Hacking Biometrics*
		30 Minuten Pause	
		11-12.30 Uhr: Diskussion der Anleitungen, danach Praxistest bis Ende	sämtliches Zubehör aus og. Anleitungen
14-15.30	Aufbau und Funktionsweise eines biometrischen Systems	gemeinsames *Resümee* mit Tafelanschrieb als Ergebnissicherung	Bausteinkarten
TAG 2 9-12.30	Technische und soziale Akteure eines biometrischen Systems	**9-9.15 Uhr:** Kurzvortrag zu Eurodac, Einführung in ein zugehöriges Rollenspielszenario auf Basis einer Pressemitteilung von Pro Asyl	Pressemitteilung PRO ASYL[567] *Akteurskarten:* Wir nehmen verschiedene Perspektiven ein: Es gibt den **Jungen**, der von der **Polizei** seine Fingerabdrücke abgenommen bekommt. Es gibt die **Ausländerbehörde** und das **Bundesamt für Migration und Flüchtlinge (BAMF)**, die abschieben will. Es gibt **Freunde,** die den Jungen gut kennen und ihn unterstützen. Es gibt die Nichtregierungsorganisation **PRO ASYL**, die zusammen mit dem **Anwalt des Jungen** die Abschiebung verhindern wollen. Weiter gibt es das **Verwaltungsgericht** mit seiner Entscheidung. Zusätzlich ist auch eine **IT-Expertin** geladen, die die Korrektheit der Ergebnisse von Eurodac anzweifelt.
			fortgesetzt auf nächster Seite

[567] Pro Asyl 2009.

Tabelle 5.3 – fortgesetzt von letzter Seite

Zeit	*Themenkomplex*	*Aktivitäten*	*Arbeitsmaterialien*
		9.15-9.45 Uhr: Aufgabe: Wählen Sie eine der Akteurskarten und bereiten Sie anhand des gegebenen Falls und Argumenten, die Sie sich selbst überlegen, kurz Ihre Rolle für eine anschließende Diskussion in einer Talkshow mit dem Thema „Sollen Computer über eine Abschiebung entscheiden?“ vor. (Recherche im Internet erlaubt) **9.45-10.30 Uhr:** Durchführung der Talkshow – Moderation durch die Dozentin mit Impulsfragen. Eine Teilnehmerin sammelt Aussagen der einzelnen Akteure in einem Protokoll.	
		30 Minuten Pause	
	Fehlerdimension II: Visualisierung der Prozesse im User- Interface / Fehlervisualisierung?	**11-12.30 Uhr:** vertiefte Analyse der GUI des SourceAFIS, der Herstellersoftware U.Are.U-4000	entsprechende Software auf den Laptops installieren; alternativ: Recherche nach Werbefilmen und Screenshots während des Workshops
14-15.30		Reflexion des Vormittags: **14-14.45 Uhr:** 1. Welche Beziehungen konnten wir zwischen den Akteuren aus dem Rollenspiel herstellen? Ergebnissicherung auf einem Plakat **14-15.30 Uhr:** 2. Diskussion und Ideensammlung Wie könnte man das Lernmodul zur Fehlervisualisierung besser gestalten?	große Papierrollen, Eddings, Kleber, buntes Papier, Scheren für die Plakaterstellung
TAG 3 9-12.30	Welche historischen Motivationen hat die Biometrie? Wie wurde sie verwissenschaftlicht? Was wurde daran automatisiert?	**9 - 9.45 Uhr:** Textlektüre anhand der Hauptfragen **9.45-10.30 Uhr:** gemeinsame Besprechung und Diskussion	Text: Cole, Simon A. (2004): *History of Fingerprint Pattern Recognition.* In: Ratha/Bolle: *Automatic Fingerprint Recognition Systems.* New York: Springer, 1-25.

Bericht und Auswertung

Der folgende Bericht ist aus den Notizen entstanden, die ich mir täglich unmittelbar nach dem Kurs gemacht habe.

Meinen geplanten Einstieg, den Teilnehmerinnen zunächst die vollautomatische Anmeldung mit dem U.are.U-Scanner, Enrolment und Visualisierungen der zugehörigen Software am eigenen Rechner zu zeigen, während sie ihre Beobachtungen auf einzelne Karteikarten notieren, verschob ich, da mir ein gesprächigerer und weniger aufgabengeleiteter Einstieg in dieser kleinen Runde angenehmer erschien. Daher zog ich den für den Nachmittag geplanten Teil vor: Mit einem Tafelbild erläuterte ich die Kom-

ponenten eines biometrischen Systems. Es folgte ein längeres Diskussionsgespräch rund um Fingerabdruckidentifizierung. Erste Begriffe („Angst“, „Bürgeramt“ bspw.), die dabei fielen, schrieb ich demonstrativ an die Tafel, strukturierte nach Akteuren und erfragte weitere Begriffe (bspw. ordnete ich das Bürgeramt unter „STAAT“ und erfragte ePass, eID und eAT, leitete auf Eurodac weiter), und es entstanden längere Diskussionen.

Nach und nach versuchte ich zum geplanten praktischen Teil überzuleiten, sprang aber zwischendurch nochmal zur Tafeldokumentation zurück.

Ich kündigte dann an, dass ich eine Anleitung zum Überlisten eines Fingerabdruckscanners mit einem Fake-Finger ausprobieren möchte, und packte all die Zutaten aus, die ich dafür geholt hatte. Auch hier: Planabweichung, kein Textstudium wie vorgesehen, sondern erste Erläuterungen meinerseits, wie ich mir das Überlistungsszenario des Fingerabdruckscanners genau vorstelle. Es zeigte sich: Das Raten, welche Rolle wohl die einzelnen Sachen spielen, schien allen Spaß zu machen.

Ich führte nun den Teilnehmerinnen die Anmeldung mit dem U.are.U-Scanner vor und erläuterte dabei auch die Unsichtbarkeiten beim Enrolment.

Dann begannen wir mit dem Abarbeiten der vorgegebenen Anleitung. Eine Teilnehmerin protokollierte – Teile dieses Protokolls fließen im Folgenden ebenfalls ein:

Die folgenden Schritte liefen teilweise durcheinander, zeitversetzt und mit vielen Unterbrechungen:

Test 1 „Creating an artificial finger using a latent fingerprint“:[568]

1. Sichtbarmachung eines latenten Fingerabdrucks:
    - Fingerabdruck auf sauberem Teller hinterlassen,
    - Fingerabdruckpulver hergestellt aus Graphitmine (Bleistift) und Babypuder,
    - Fingerabdruck mit dem hergestellten Pulver zugedeckt, überschüssiges Pulver mit dem Pinsel entfernt,
        - erste größere Probleme:
            * Babypuder mit Bleistiftgraphit gemixt schien auf weißem Untergrund zu matt. Es war sehr viel Fingerspitzengefühl erforderlich. Das Auftragen des Pulvers mit dem Pinsel ging noch gut, das Wegnehmen mit dem Pinsel aber führte eher zum Entfernen des gesamten Puders. Allerdings war der mit dieser Pulvermischung hergestellte latente Abdruck noch der sichtbarste (allerdings weniger sichtbar als mein Test zu Hause nur mit Graphitpulver).

[568] Kaseva und Stén 2003c.

    - * *andere Variante*: Tonerreste (Magenta); Nachteil: giftig. Wir probierten es dennoch, da es auf dem Foto der Anleitung sehr vielversprechend aussah. Doch mit dem Pinsel das überschüssige Pulver zu entfernen ging hier noch schlechter. Wegpusten war besser, aber da der Staub ungesund ist, wollten wir das nicht lange machen.

2. Erstellen eines Fotos des sichtbar gemachten Fingerabdrucks:
    - Hierbei traten viele Probleme auf:
        - die Lichtverhältnisse im Raum waren zu schlecht, das einzige Foto, was gut gelang, haben wir am Fenster gemacht,
        - Fingerabdruck auf der Innenseite eines tiefen Tellers: es traten Schwierigkeiten beim Fotografieren auf wie Schatten, Reflektionen,
        - je nach Farbe des Untergrunds empfahl es sich, dunkleres oder helleres Pulver zu nehmen,
        - Fingerabdruck auf nicht oder wenig reflektierender Oberfläche nehmen,
        - evtl. Tesafilm verwenden.

Den ersten Test brachen wir an dieser Stelle ab, da die Fotos eine zu schlecht erscheinende Qualität für eine weitere digitale Nachbearbeitung hatten.

Test 2 „Creating an artificial finger using the actual finger“:[569]

- mit einer Heißkleberpistole eine kleine Menge Kleber (ca. 3x3cm) auf ein Blatt Papier setzen,
- ein paar Minuten warten, bis der Kleber abgekühlt ist (gute drei bis vier Minuten!, sonst wurde es schmerzhaft),
- Finger ca. eine Minute in die noch weiche, aber genügend abgekühlte Klebermasse eindrücken, dann komplett abkühlen lassen,
- Gelatine vorbereiten: Aufquellen lassen, Ausdrücken, Kelle mit ausgedrückter Gelatine über Wasserbad halten und solange rühren, bis die Gelatine flüssig ist,
- Gelatine in die Form gießen und warten, bis sie abgekühlt ist (Kühlschrank empfehlenswert – Dauer 15 Minuten).

[569] Kaseva und Stén 2003b.

Obwohl die Form hervorragend wurde, gelang es nicht, darin einen gut haltbaren Gelatine-Überzug für den Finger zu produzieren, der beim Auflegen auf den Scanner hielt. Vermutlich hatten wir ihn zu sehr zerdrückt beim ersten Auflegen oder er war zu kalt, zu trocken, zu hart. Aus meiner Sicht gab es dadurch keine wirklichen Erfolgserlebnisse mit Ablauf des ersten Tages.

Alle waren ein bisschen frustriert. Gleichzeitig war aber von vornherein klar, dass das Experiment misslingen könnte, da der Workshop ja ein erster Probelauf sein sollte. Der Scanner war bis zu diesem Zeitpunkt noch nicht einmal erfolgreich gehackt worden. Es sollte also unbedingt in irgendeiner Form sichergestellt sein, dass im Rahmen der gegebenen Zeit Ergebnisse sichtbar sind, die als Erfolg gewertet werden können – bei einem Experiment mit unbekanntem Ausgang sollten auch die Zwischenergebnisse klarer als erfolgreiche Ziele gesteckt werden und klare Teilphasen erkennbar sein.

Die Wiederholungen verschiedener Zwischenschritte und die Suche nach Alternativen bei nicht zufriedenstellenden Zwischenergebnissen erforderten viel Zeit. Zudem waren beispielsweise Kühlzeiten, Wege zu Wasserhähnen, das Besorgen von fehlenden Materialien wie dem Toner sehr zeitintensiv. Auch das Fotografieren will gekonnt sein – die Suche nach den richtigen Einstellungen des Fotoapparats und vor allem geeigneter Beleuchtung waren frustrierend. Es zeigte sich bereits hier, dass für ein maßgeschneidertes Praxis-Lernmodul zu Überwindungstests eine enorme Vorbereitung nötig ist, um das in der anfangs vorgestellten Zeit von maximal zwei 90-Minuten-Blöcken umsetzen zu können. Im Grunde ist der gesamte praktische Teil eine äußerst heikle Angelegenheit, bei der den Teilnehmenden sehr viel Eigeninitiative abverlangt wird und sich die Dozentin stark zurücknehmen können sollte.

Die verbliebene Teilnehmerin und ich einigten uns darauf, es am Folgetag nochmals mit der Anleitung des Chaos Computer Clubs zu versuchen, die durch einen begleitenden Film und wesentlich weniger Materialaufwand machbarer erschien. Außerdem wechselten wir den Raum, da wir für die Fotos eine hellere Umgebung brauchten. Der Raumwechsel war zeitintensiv, aber lohnte sich lichttechnisch.

Zur Sichtbarmachung der Fingerabdrücke nutzten wir diesmal Graphitpulver, mit dem wir wesentlich bessere Ergebnisse als am Vortrag erzielten, da es auch bei nicht ganz so sanftem Pinseln klarere Bilder ergibt. Dennoch musste man hier sehr, sehr vorsichtig sein. Es ging auch mit zaghaftem Pusten – eine Idee der Teilnehmerin war hier, es vielleicht mit einem Strohhalm zu versuchen. Wir nutzten diesmal neben Geschirr als Untergrund auch Glas (wie im Video des CCC) – das bedeutete für die Fotografie allerdings ebenfalls eine gewisse Herausforderung.

Mit den Dämpfen des Sekundenklebers konnten wir den latenten Abdrucks nicht sichtbar machen. In den späteren Versuchen in der Schule oder beim Uni-Seminar zeigte sich aber: Wenn der Sekundenkleber Cyanoacrylat enthält und die Dämpfe *mindestens* eine Minute mit einem leicht formbaren Gummideckel oder ähnlichem so luftdicht wie möglich abgeschlossen an den Abdruck gelangten, dann funktionierte es.

Wir produzierten durch die besseren Beleuchtungsverhältnisse und die Erfahrung mit der Kamera viel bessere Bilder als am Vortag.

Das nächste zeitintensive Problem stellte die korrekte Nachbearbeitung der Bilder dar. Laut Stén/Kaseva sollten das Abschneiden der Bildreste, die nicht zum Fingerabdruck gehörten (quasi eine manuelle Segmentierung), das Erhöhen des Kontrasts („so that the print has a clear pattern“[570]) und die korrekte Skalierung ausreichen, aber sobald die Beleuchtung nicht gleichmäßig war, wurde die Kontrastierung unterschiedlich stark. Der Glasuntergrund war auch zu wechselhaft. Ein klares Muster war nie zu erkennen. Wir arbeiteten weiter mit Tonwertkorrekturen, Binarisierung und schließlich Invertierung. Es wurde schnell klar, dass auch zuviel Nachbearbeitung die Bilder schnell zerstören kann. Der nächste Schritt war die Skalierung des Abdrucks auf seine korrekte physische Größe für den Ausdruck, die durch Veränderungen in den Bildauflösungen verfälscht werden kann. Dazu müssen eigentlich schon vor dem Fotografieren zwei Fixpunkte am Abdruck markiert werden, deren Abstand man mit einem Lineal messen kann und dann im Bildbearbeitungsprogramm wie Photoshop oder Gimp genau übernimmt.

Innerhalb dieses gesamten geschilderten Prozesses simuliert man per Hand viele Bildbearbeitungsschritte, die im biometrischen System automatisch passieren, und kann hier praktisch erleben, welche Probleme alles auftauchen können, erstens, wenn bereits am Sensor eine schlechte Bildvorlage produziert wird und, zweitens, wenn die Nachbearbeitungsschritte nicht ausgewogen auf mögliche Sensorbilder abgestimmt sind, indem die Bildqualität sinnvoll gemessen wird.

Es ging weiter: Die nachbearbeiteten Fingerabdruckbilder haben wir schließlich in verschiedenen Größen ausgedruckt, mit Holzleim bestrichen, den wir nach Trocknung abgezogen und auf die Fingerkuppen gesetzt haben. Während wir keine erfolgreiche Erkennung mit einem bereits gespeicherten Abdruck erreichen konnten, konnten wir zumindest den gefälschten in einem Enrolment einlesen. Es war also lediglich möglich, mit dem Fingerabdruckscanner einen gefälschten Abdruck neu zu registrieren und diesen auch zu verifizieren. Allerdings nutzten sich die Leim-Abdrücke auch schnell ab.

Da wir letztlich keinen komplett erfolgreichen Überwindungstest durchführen konnten, blieb diesbezüglich am Ende eine gewisse Frustration. Doch es ist ein Experimental-Setting, bei dem auch das Nicht-Gelingen ein wertvolles Ergebnis ist. Wir erstellten eine Abschlussdokumentation als Plakat, in der wir die Anleitung des CCC um eine Benennung der Fallstricke bereicherten. Außerdem verdeutlichten wir in diesem Zusammenhang die politisch-soziale Dimension, indem wir die Akteursbeziehungen, die im Geflecht um biometrische Systeme entstehen, dokumentierten.[571] An

[570] Kaseva und Stén 2003c.

[571] Siehe Anhang *Plakat »Sicherheits-industrieller Komplex«, Informatica Feminale.*

dieser Stelle floss ein Aspekt aus der ursprünglichen Planung ein, nämlich der Teil, den ich mit dem Rollenspiel abdecken wollte.

Der Workshop war oft improvisiert und hatte mit der ursprünglichen Planung wenig gemein – allerdings war dies angesichts der aufwändigen Umsetzung des erstmalig vollständig durchgeführten Experiments und des Ausbleibens einer ausreichenden Anzahl von Teilnehmenden angemessen. Gemäß der Rückmeldung in der Evaluation der Veranstaltung empfand die Teilnehmerin den Workshop eher schlecht vorbereitet. Das sonstige Feedback war aber positiv: Die Anforderungen und Lehrinhalte wurden als angemessen empfunden, die Erwartungen größtenteils erfüllt, das Verhältnis von Theorie und Beispielen/Übungen als größtenteils ausgewogen und die Vorabinformationen als ausreichend sowie die Gliederung des Ablaufs als größtenteils sinnvoll bewertet. Die Lernatmosphäre wurde als angenehm und entspannt empfunden. Insbesondere die Ergebnissicherung auf der Plakatwand war gut gelungen und ermöglichte uns, auch den anderen Besucherinnen der Sommeruniversität über die Inhalte des Workshops zu berichten und mit ihnen ins Gespräch darüber zu kommen – bei dem inhärenten politischen Anliegen war dies ein wichtiger Erfolg.

5.3.2 Unterrichtsreihe am Oberstufenzentrum Handel 1, Berlin, 2012

Für die nächste Erprobung des Lernprojekts, inzwischen mit dem Titel »Überwachungstechnologien begreifen: Wa(h)re Identität und der Fingerabdruck«, wählte ich einen schulischen Rahmen. Hierfür wendete ich mich an den Informatik-Lehrer Johann Penon am Oberstufenzentrums Handel 1 in Berlin-Kreuzberg (OSZ Handel 1).[572] Die Arbeitsgruppe »Informatik in Bildung und Gesellschaft« hatte sowohl durch die Ausrichtung von Tagungen der Fachgruppe »Informatik-Bildung in Berlin und Brandenburg« (IBBB) der Gesellschaft für Informatik sowie die langjährige Zusammenarbeit in der schulpraktischen Ausbildung der Lehramtsstudierenden der Informatik an der Humboldt-Universität zu Berlin gute Kontakte zu engagierten Lehrern des OSZ Handel 1. Insbesondere die dortigen (inzwischen ehemaligen) Informatik-Lehrer Siegfried Spolwig und Johann Penon haben sehr erfolgreiche Unterrichtsprojekte, Aufgaben und Übungen entwickelt und online zur Verfügung gestellt und wichtige Beiträge zur Fachdiskussion der Informatikdidaktik geliefert.[573]

Das im Jahr 1979 gegründete OSZ Handel 1 ist eine der größten deutschen Wirtschaftsschulen mit zur Zeit ca. 4.700 Schülern und 221 Lehrern.[574] Es besitzt eine vierzügige gymnasiale Oberstufe und beherbergt zusätzlich eine Fachoberschule und eine

[572] http://www.oszhandel.de, letzter Abruf: 30.7.2017.

[573] Vgl. u. a. Penon und Spolwig 1994. Die Online-Datenbank http://videocenter.schule.de (letzter Abruf: 30.7.2017) wird bis heute durch Johann Penon gepflegt und kann für den Schulunterricht zu relationalen Datenbanken hervorragend genutzt werden. Weitere: Penon und Spolwig 1998, Witten, Penon und Dietz 2006.

[574] Siehe http://www.oberstufenzentrum.de/schulen/osz-handel-i, letzter Abruf: 30.7.2017.

Berufsfachschule. Ein besonderes in Berlin einmaliges Angebot ist der Leistungskurs Wirtschaftsinformatik in der gymnasialen Oberstufe. Innerhalb dieses Leistungskurses wurde mir nach Einreichung meines im *Kapitel 5.2 Konzeption eines Lehr- und Lernprojekts zur Fingerabdruckerkennung* vorgestellten Konzepts gestattet,[575] im Profilkurs (11. Klasse) des Informatik-Lehrers und Fachbereichsleiters Thomas Lingens eine fünfwöchige Unterrichtsreihe vom 29. Oktober bis 28. November 2012 durchzuführen.

Lern- und Lehrvoraussetzungen

Im Folgenden werden die wichtigsten infrastrukturellen Rahmenbedingungen für die Durchführung des Kurses und Lernvoraussetzungen bei den Schülern erläutert.

Zunächst besprach ich ich mit dem Kurslehrer mein Lehrkonzept. Er habe es gelesen, sehr interessant gefunden und lange darüber nachgedacht, in welchem der beiden Leistungskurse er es mich durchführen lassen wolle. Schließlich entschied er sich für den Wirtschaftsinformatik-Leistungskurs, der sich im ersten Kurshalbjahr befand. Da passe es thematisch zwar eigentlich gerade nicht, aber die Schülerinnen seien sehr motiviert, während sein drittes Kurshalbjahr „so lätschig" sei, das wolle er mir nicht antun. Für die komplette Durchführung bekam ich freie Hand – allerdings musste eine Klausur geschrieben werden, die ich in Absprache mit ihm konzipieren sollte, die aber von ihm bewertet wurde. Der Kurslehrer stand mir von da an auch weiter insgesamt sehr freundlich und hilfsbereit zur Seite und gab viel Feedback.

Die Unterrichtsreihe wurde also im Leistungskurs „Wirtschaftsinformatik", 1. Halbjahr (12. Klasse) ungefähr in der Schuljahresmitte gegeben. Von den wöchentlich fünf Stunden, die der Leistungskurs Unterricht in diesem Fach hat, übernahm ich zwei Blöcke à 90 Minuten – einmal am Montag zwischen 11.40 und 13.10 Uhr (5./6. Stunde), also nachdem die Schülerinnen bereits zwei solcher Blöcke hinter sich hatten, den zweiten am Mittwoch zwischen 9.50 und 11.20 Uhr (3./4 Stunde). Diese Stunden fanden in einem der für den Informatik-Unterricht ausgestatteten Räume statt. In der Mitte des Raumes waren die Tische so gruppiert, dass sich alle Schülerinnen einander zugewandt um eine große Tischfläche setzen konnten. Circa 20 Arbeitsrechner standen u-förmig an drei äußeren Wänden des Raumes mit rollbaren Stühlen, so dass Phasen des Einzel- oder Teamlernens am Computer klar von anderen Unterrichtssequenzen am „Konferenztisch" abgetrennt werden konnten und für Unterrichtsgespräche eine geeignete seminaristische Atmosphäre herrschte.

Im Raum gab es Beamer, Whiteboard und einen eigenen Rechner für den Lehrer. Eine zentrale Abschaltung der Bildschirme an den Arbeitsplätzen durch die Lehrerin war möglich. Der Internet-Zugang für die Schülerinnen war unbeschränkt. Alle Rechner waren mit Windows XP Teil eines schuleigenen LAN mit klar strukturierten Rechtevergaben, die Veränderungen an der Systemkonfiguration oder Installationen im regu-

[575] Eingereichte Fassung siehe Anhang *Eingereichtes Unterrichtskonzept OSZ Handel I.*

lären Lehrbetrieb unmöglich machten. Der mich unterstützende Kursleiter bat mir an, für mein Projekt zusätzlich zu installierende Software nach Vorgaben meinerseits im Vorhinein selbst zu installieren. Auch zum Raum bekam ich keinen eigenen Zugang. Ich wurde vor Beginn der Unterrichtsreihe dem Schulleiter, der Abteilungsleiterin, dem Systemadministrator und ein paar Kollegen bei einem kurzen Treffen vorgestellt.

Um die im Unterricht verwendeten digitalen Materialien verfügbar zu machen, erhielt ich einen Zugang zum Lernmanagementsystem *Moodle*, das die Schule nutzt.

Der Kurs bestand aus 16 Schülern, von denen vier Mädchen und zwölf Jungen waren. Bei einer vorhergehenden Hospitation am Montag, den 22.10.12, machte ich mir einen ersten Eindruck von der Klasse. Mir fiel auf, dass die Mädchen im ganzen Raum verteilt zwischen den Jungen saßen. Sie wirkten alle keinesfalls schüchtern – einen Eindruck, den ich häufig bei Hospitationen in Informatikkursen der Sekundarstufe 2 an verschiedenen Schulen hatte. Es gab zwei, drei sehr extrovertiert wirkende junge Männer, die gern auch etwas provokanter gegenüber ihrem Lehrer auftraten. Nach dem, was im Laufe des Kurses von den Schülern an Geschichten erzählt wurde, erschien mir die Gruppe auf einen sogenannten „Migrationshintergrund“ bezogen als sehr heterogen – viele haben vermutlich Eltern oder Großeltern, die nicht in Deutschland groß geworden sind. Einige der Schüler hatten bereits eine Berufsausbildung hinter sich, so dass es auch eine heterogene Altersstruktur gab. Zudem kommen die Schüler an einem beruflichen Gymnasium in der Regel aus 10. Klassen von Sekundar-, Gesamtschulen und Gymnasien und sind nicht zwangsläufig von der „Monokultur“ eines rein gymnasialen oder gar elitären Selbstverständnisses geprägt.

Das Thema der ersten Hälfte des Schulhalbjahres war bis dahin IT-Projektmanagement gewesen, in der hospitierten Stunde ging es um Geschäftsprozesse. Einzelne Gruppen präsentierten mit Power-Point-Folien, was sie dazu erarbeitet hatten. Die sprachlichen Fähigkeiten und die Art der Präsentation hatten in der Mehrheit ein hohes Niveau – aus meiner Sicht für den schulischen Kontext schon erstaunlich professionell. Zudem wirkte die Mehrheit der Schülerinnen relativ engagiert. Die Atmosphäre wechselte zwischen größerer Unruhe und relativ aufmerksamem Zuhören. Nur Einzelne wirkten abwesend und abgelenkt.

Der Notenschnitt einer zurückgegebenen Klausur lag laut dem Kursleiter bei 2,7, davon keine Fünf, zwei Einsen, zwei Zweien. Das Niveau der (informatischen) Vorkenntnisse und der Fähigkeiten, Gelerntes zu behalten, es anzuwenden, in Zusammenhänge einzuordnen, zu abstrahieren und mit strukturierten Argumentationen zu diskutieren sollte ich erst im weiteren Verlauf besser abschätzen können.

Die prinzipielle Motivation der Schülerinnen für die Beteiligung am Unterricht schätzte ich als relativ hoch ein, da im Rahmen der Abiturphase in den pflichtgemäß zu belegenden Leistungsschwerpunkten der konkrete fachlich-inhaltliche in einem gewissen Rahmen frei gewählt werden kann. Die Schule wirbt zudem insbesondere mit dem Angebot von Wirtschaftsinformatik als Leistungsfach.

Meine Unterrichtsreihe ließ sich an das Thema IT-Projektmanagement insofern anschließen, als dass auch ein biometrisches System im Rahmen typischer Design-Prozesse entsteht, bei denen Anforderungen der Kundinnen erhoben und in einer Reihe von Entwurfsphasen umgesetzt werden. In den Inhalten des Lernprojekts kam dies im Rahmen der Interessenskonflikte verschiedener Akteure bezogen auf Überwachungssysteme zum Tragen.

Planung der Unterrichtsreihe gesamt

Den Verlauf der gesamten Reihe – insgesamt 18 Stunden Unterricht sowie zwei Stunden Klausur – plante ich insgesamt wie in Tabelle 5.4 dargestellt:

Tabelle 5.4: Gesamtplanung der Unterrichtsreihe am OSZ Handel 1.

Datum	Stunde	Thema
Mo, 29.10.12	1. Stunde	Kennenlernen und Einstieg: *Worum geht es?* *Was ist ein biometrisches System?* (Brainstorming/Mind-Map)
	2. Stunde	Spiel „Analoge Finger-Biometrie“
Mi, 31.10.12	3. Stunde	Rekapitulation letzte Stunde, Mindmap Biometrie, Komponenten zusammenlegen
	4. Stunde	eAT-Film vom BAMF (Kritik und Diskussion)
Mo, 5.11.12	5. Stunde 6. Stunde	Einstieg und Vorbereitung Fake-Finger-Produktion
Mi, 07.11.12	7. Stunde 8. Stunde	Fortsetzung Fake-Finger-Produktion
Mo, 12.11.12	9. Stunde 10. Stunde	Textarbeit: Technik, Geschichte, Kritik, Glossar
Mi, 14.11.12	11. Stunde 12. Stunde	Einstieg mit Begriffsquiz, Vorträge zu den Texten und gegenseitige Kritik
Mo, 19.11.12	13. Stunde 14. Stunde	KLAUSUR
Mi 21.11.12	15. Stunde	Modellieren und Entwickeln – Entwicklung eines Beispielalgorithmus mit Hilfe eines Programmablaufplans o. ä.
	16. Stunde	erste Begegnung mit sourceAFIS
Mo, 26.11.12	17. Stunde 18. Stunde	sourceAFIS - GUI und Bearbeitung Beispielalgorithmus
Mi, 28.11.12	19. Stunde 20. Stunde	Diskurs Biometrie: Werbung, Studien, Benchmarks

Mit dem Einstieg über ein allgemeines Brainstorming zum Thema Biometrie möchte ich zunächst sammeln, welches Vorwissen, welche Einschätzungen oder aufgeschnappten Fakten, Ideen oder Assoziationen bei den Schülerinnen vorhanden sind. Hiermit wird das Feld sehr breit eröffnet – die Schülerinnen richten sich gedanklich auf Anwendungen aus, die sie mit automatischer Fingerabdruckerkennung verbinden. Für erste Überlegungen, worin genau der technische Vorgang einer solchen Fingerabdruckerkennung besteht, folgt dann eine praktische, lockere Nachstellung der traditionellen Fingerabdruckabnahme und der Abgleich mit sichtbar gemachten latenten Abdrücken. Hier gibt es im Spielwarenhandel Detektivspiele mit vereinfachtem forensischen Werkzeug und kleinen Kriminalgeschichten, die inspirieren können. Begleitend zum Spiel sollen erste strukturierende Überlegungen gemacht werden: Aus welchen Bestandteilen müsste so ein Fingerabdruckerkennungssystem bestehen, wenn es die gerade probierte manuelle Tätigkeit übernehmen soll? Welche Probleme treten eigentlich beim Vergleichen auf, welche Fehler sind dabei möglich?

Im nächsten Block werden dann die Überlegungen der Stunde zuvor systematisch in die Bestandteile eines generischen Systems überführt, Grundbegriffe werden eingeführt. Die vermutlich schon in der Mind-Map in Form von Filmen oder realen lebensweltlichen Anwendungen angeklungenen Aspekte des Kontexts eines solchen Biometrie-Systems werden dann im zweiten Teil nochmal aufgegriffen und mit einer Fokussierung auf eine konkrete Anwendung, in diesem Fall den Fingerabdruck im elektronischen Aufenthaltstitel (eAT), anhand eines Werbefilms dafür illustriert. Schon frühzeitig wird die technische Anwendung hier konkret auch ethisch geprüft und diskutiert – insbesondere soll erörtert werden, welche Erfahrungen mit dem Fingerabdruck im Ausweisdokumenten bestehen, warum sie bei Ausländerinnen Pflicht sind, bei Staatsbürgerinnen (noch) nicht? Wozu dienen die Fingerabdrücke? Welche Rolle spielt in diesem Zusammenhang Sicherheit, wessen Sicherheit vor wem oder was?

Anknüpfend an den wichtigen Aspekt der Sicherheit, der im Fallbeispiel der letzten Stunde ein Thema gewesen ist, eröffnen die darauf folgenden zwei Blöcke die Problematik der Fälschungssicherheit des Fingerabdrucks. Da gerade hier ein besonderer kritischer Diskurs ansetzt, soll genauer praktisch geprüft werden: Wie fälscht man einen Fingerabdruck eigentlich?

Daran anschließend wird wieder eine theoretische Systematisierung stattfinden und zudem auch die historische Perspektive auf das Thema erweitert. Es wird rekapituliert, welche technischen Begriffe rund um Aufbau und Funktionsweise eines automatischen Fingerabdruckerkennungssystems nötig sind (Aufbau eines Glossars). Mit Hilfe der Methode des Gruppenpuzzles sollen nun sowohl mit Hilfe eines Texts dazu die historische Rolle des Fingerabdrucks in der Kriminaltechnik und der Kritik daran behandelt und diskutiert sowie aktuelle bürgerrechtliche Kritik an der Ausweitung der biometrischen Praktiken damit in Beziehung gesetzt werden. Im Rahmen des Gruppenpuzzles soll ermöglicht werden, dass jeweils einige Expertinnen für ausgewählte The-

menbereiche allen anderen soviel darüber beibringen, dass jede theoretisch zu einem der erarbeiteten Themen befragt werden kann. Mit einem Begriffsquiz, Vorträgen zu den verteilten Texten und gegenseitiger konstruktiver Kritik werden die Ergebnisse dieser Arbeiten in einem weiteren Block gefestigt.

Nach der Klausur soll es nun erstmalig um die Software-Modellierung von Komponenten eines biometrischen Systems gehen. Um gleichzeitig auch auf wichtige Modellierwerkzeuge der Softwareentwicklung zurückzugreifen, ist auch die Auseinandersetzung mit Darstellungen ausgewählter Algorithmen in Prozess- oder Unified-Modeling-Language-(UML)-Diagrammen geplant. Anhand von SourceAFIS soll eine erste Code-Analyse gemacht werden: Wie sehen die Implementierungen der Softwarekomponenten auf Code-Ebene aus? Wo finden wir Konstanten, die den Ablauf des Vergleichs zweier Templates verändern? Zudem soll die GUI geprüft werden. Was wird dort wieso veranschaulicht? Die Begegnung mit der Software auf Development-Ebene ist nur für zwei Blöcke geplant und soll explizit auch eine vielleicht für viele erste Begegnung mit klassischen Tools der Programmierung sein (Editoren, Entwicklungsumgebungen, Kommandozeile, Compiler, Interpreter). Hier werden die Schülerinnen vielleicht am stärksten in das kalte Wasser der wenig anschaulichen Teile der Informatik geworfen – es soll aber der Versuch sein, genau zum bastelnden, experimentierenden, demontierenden Bestreben des Hackens zu motivieren: „Wenn ich in die Black Box reinschauen will, muss ich irgendwie auch an den Code ran."

Schließlich wird im letzten Block nochmal alles bisher rund um ein Biometrie-System Entdeckte – theoretisches Begriffsrepertoire, Modelle, Einbettung in die Lebenswelt, Geschichte, Software- und Hardwarerealität konkreter Anwendungen – als diskursives Gebilde in den Blick genommen. Anhand von Werbungen, Studien oder Benchmarks soll gefragt werden: Was spiegelt sich von dem, was gelernt wurde, in dem wider, was darüber verkauft oder berichtet wird?

Diese Gesamtplanung habe ich in der konkreten Realisierung teilweise nach und nach verändert, an das Lerntempo oder sich entwickelnde Bedürfnisse angepasst. Zwei konkrete Stundenverlaufsplanungen – die der ersten zwei Blöcke – finden sich in Tabelle 5.5 und Tabelle 5.6 und werden im nächsten Kapitel in ihrer durchgeführten Umsetzung besprochen.

Tabelle 5.5: Verlaufsplanung 1./2. Stunde. In der Tabelle verwendete Abkürzungen: S: Schülerinnen, L: Lehrender, UG: Unterrichtsgespräch

Phase	Zeit	Aktionen	Sozialform	Arbeitsmittel	Aufgabenstellung
Einstieg/ Kennenlernen	11:40	L eröffnet Stunde mit kurzer Selbstvorstellung und den ersten 2 Folien, teilt dann die Gruppen ein: 4 x 4 S	Frontalvortrag, Gruppenverteilung	Gruppenkarten (A1..4 bis E1..3), Folien 1-3 / Beamer, Schüler: Notizzettel oder Hefter	

fortgesetzt auf nächster Seite

Tabelle 5.5 – fortgesetzt von letzter Seite

Phase	Zeit	Aktionen	Sozialform	Arbeitsmittel	Aufgabenstellung
	11:45	S machen kurze Interviews innerhalb ihrer durch die Gruppenkarten gemixten Vierer- oder Dreiergruppen und notieren sich die zentralen Begriffe, währenddessen bereitet L Whiteboard vor	Gruppenarbeit	S: Notizzettel oder Hefter	„Besprechen Sie sich kurz untereinander in der Gruppe und bereiten Sie eine Vorstellung eines jeweils anderen Gruppenmitglieds und eines Begriffs für das Brainstorming vor: (A) Warum hat sie oder er den Informatik-Kurs gewählt? (B) Welche Begriffe, Filme oder Bilder fallen ihr/ihm zum Titel der Unterrichtsreihe der nächsten vier Wochen ein: „Überwachungstechnologie begreifen: Wa(h)re Identität und der Fingerabdruck“?“
	12:05	S-Gruppen stellen einander vor und einer aus einer anderen Gruppe schreibt am Whiteboard mit	Schülerpräsentation		
Erarbeitung	12:15	In jeder Gruppe wird eine Person gewählt, die ihren Fingerabdruck des rechten Daumens auf einer Fingerabdruckkarte abgibt. Es wird weiterhin ein Pseudonym darauf vermerkt, das die Person benutzt. Die Personen, die Fingerabdrücke gegeben haben, ziehen sich kurz zurück und hinterlassen Fingerabdrücke auf den Beweisstücken. Währenddessen untersuchen die anderen ihre Abdrücke genauer. Jede Gruppe erhält ein Beweisstück und soll die Täterin finden.	Gruppenarbeit	6 FA-karten (2 bitte 30x kopieren!), 5 Kopien aus der Anleitung, 5 Kopien Klassifikationsanleitung, 1 Stempelkissen (4 weitere besorgen!), 5 Pinsel, 5 Lupen, 3 kleine Teller, Zellstoff zum Abwischen, Klebeband, Zeitungspapier zum Unterlegen, 4 Fl. Graphitpulver	„1. Wählen Sie in Ihrer Gruppe jemanden aus, dessen/deren Fingerabdrücke vom rechten Daumen und Zeigefinger Sie auf einer Fingerabdruckkarte nehmen. Notieren Sie außerdem ein Pseudonym, das die Person selbst wählt als Namen für diese Person. Die Person geht von Gruppe zu Gruppe und gibt jeweils ihre beiden Abdrücke mit dem Stempelkissen dort ab. Schauen Sie sich die erzeugten Fingerabdrücke mit der Lupe an. 2. Klassifizieren die Grundmuster und zählen Sie die Minutien, notieren Sie die Besonderheiten (Narben, Falten z. B.) anhand des Klassifikationsblattes.
					fortgesetzt auf nächster Seite

Tabelle 5.5 – fortgesetzt von letzter Seite

Phase	Zeit	Aktionen	Sozialform	Arbeitsmittel	Aufgabenstellung
					3. Nehmen Sie die latenten Fingerabdrücke von den Beweisstücken auf eine weitere Fingerabdruckkarte und vergleichen Sie sie mit denen in Ihrer Kartei. Finden Sie den richtigen und schreiben Sie die Probleme dabei auf.“
Festigung/ Reflexion	12:50	Vorstellung der Ergebnisse, Zusammentragen der Probleme	UG	Beamer / Folien	
		Zusammentragen der Schritte eines biometrischen Erkennungsprozesses	UG		
Ergebnissicherung	13:00	Übernahme unklarer Begriffe und der Schritte in den Hefter	selbständig	S: Hefter	

Tabelle 5.6: Verlaufsplanung 3./4. Stunde. In der Tabelle verwendete Abkürzungen: S: Schülerinnen, L: Lehrende, UG: gemeinsames Unterrichtsgespräch

Phase	Zeit	Aktionen	Sozialform	Arbeitsmittel	Aufgabenstellung
Einstieg	9:50	L präsentiert Mind-Map mit eingebauten Tafelanschriften der S vom letzten Mal	Frontalvortrag	Mind-Map, Beamer	
Wiederholung	9:55	Komponenten eines biometrischen Systems werden rekapituliert, gemeinsam zusammengelegt	Arbeit in der großen Gruppe, UG	Komponentenkarten	„Ordnen Sie gemeinsam die vorgegebenen Komponenten zu einem Modell eines biometrischen Systems.“
	10:00	Definitionen des Begriffs „Biometrie“		UG	
Ergebnissicherung	10:10	S übernehmen das Komponentendiagramm in ihren Hefter	Einzelarbeit	S: Notizzettel oder Hefter	
Einstieg	10:20	Anschauen des Werbe-Films vom BAMF zum eAT (ca. 8:40) S machen sich Notizen zu den Beobachtungsfragen	Einzelarbeit	Film mit Beobachtungsaufträgen S: Notizzettel oder Hefter	Machen Sie sich während des Films Notizen zu folgenden Fragen: „Welche einzelnen Komponenten des biometrischen Systems sind sichtbar? Welche Informationen erhalten Betroffene von dem System? Können Sie sich Probleme und Fehler vorstellen? Sammeln Sie diese.“
Erarbeitung	10:30	Diskussion der Fragen	Diskussion		

fortgesetzt auf nächster Seite

Tabelle 5.6 – fortgesetzt von letzter Seite

Phase	Zeit	Aktionen	Sozialform	Arbeitsmittel	Aufgabenstellung
	11:00	Aufforderung zur vertieften Auseinandersetzung mit vergleichbaren hoheitlichen Biometrie-Anwendungen (ePass, Eurodac)	stille Einzelarbeit	S: Notizzettel/ Hefter	

Bericht und Reflexion der gesamten Durchführung

Bevor ich insgesamt Bilanz zur durchgeführten Unterrichtsreihe ziehe, möchte ich zwei detaillierte Berichte, die ich kurz nach Durchführung der oben in ihrer Planung vorgestellten Beispielstunden erstellt habe, hier einfügen. Sie sollen etwas von meinem unmittelbaren Eindruck bezüglich der Durchführung wiedergeben. Auf eine ausführliche Dokumentation aller Stunden wird allerdings verzichtet, da dies hier den Rahmen sprengt und viele Schlüsselerfahrungen schon mit den beiden Beispielberichten abgebildet sind.

Bericht und Resümee zum Ablauf der 1./2. Stunde Der erste Block erforderte mit seinem praktischen, materialreichen Ansatz für den manuellen Fingerabdruckvergleich diverse Besorgungen, die recht viel Zeit benötigten. Ich kam daher nahezu punktgenau mit dem Klingeln. Dementsprechend fing die Stunde leicht verspätet an, aber es schien nicht sonderlich aufzufallen. Der Kurslehrer half mir, die etwas träge Gruppe an den Konferenztisch zu holen. Ich stellte mich auf Nachfrage namentlich vor. Die Gruppenbildung moderierte ich mit Kärtchen.

Nachdem die Aufgaben für das Kennenlernspiel mit gegenseitigen Interviews zur Motivation zum Kurs und Brainstorming zum Seminartitel bekanntgegeben waren, wurde es etwas unruhig, aber alle beschäftigten sich mehr oder minder motiviert mit der Aufgabe. Sie präsentierten sich anschließend gegenseitig und ein Gruppenmitglied schrieb zentrale Begriffe des Brainstormings an. So lernte ich die Namen der Schülerinnen kennen, erfuhr ihre Interessen und warum sie in dem Kurs sind, was mich ihre grundsätzliche Motivation besser einschätzen ließ. Ich fühlte erstmalig vor, was sie mit Biometrie anfangen können. Der Kurslehrer kritisierte später am Brainstorming, dass ich den Tafelanschrieb im weiteren Verlauf der Stunde nicht mehr aufgriff. Ich selbst hatte das Gefühl, dass eine sinngebende Verknüpfung von den Kennenlernfragen und dem Brainstorming fehlte.

Danach wurde ich nach meiner eigenen Motivation zum Informatik-Studium gefragt. Bemerkenswert war, dass ein Schüler sagte, dass ich als Frau doch eine Seltenheit in dem Bereich sein müsse. Die Mädchen hielten sich komplett zurück, während ich sagte, dass es zwar tatsächlich wenig Frauen gebe, sich dies aber derzeit allmählich ändere.

Während der Gruppenarbeit der ersten Runde bereitete ich noch Teile des Materials für die nächste praktische Aufgabe vor. Hier zeigte sich, dass eine sorgsame Anordnung des vielen Materials eine halbe Stunde vor Unterrichtsbeginn sowohl für die eigene Ruhe als auch, um besser für Fragen während der Gruppenarbeit zur Verfügung zu stehen, vorteilhafter gewesen wäre.

Es ging jetzt um die Gruppenaufgaben für Abnahme, Vergleich und Zuordnung von Fingerabdrücken Einzelner in den verschiedenen Gruppen. Die Aufgaben waren an die Wand projiziert, aber es gab in den einzelnen Gruppen viele Fragen dazu. So hielt ich mich verschieden lange bei einzelnen Gruppen mit Erklärungen auf, wie die Abdrücke zu nehmen sind, versuchte, einer wartenden Gruppe eine andere Methode der Fingerabdruckabnahme mit dem Pulver und dem Klebeband zu zeigen, sie probierten es. Als die erste Gruppe fertig war, begann ich zur dritten Aufgabe zu springen, um sie beschäftigt zu halten. Sie sollten einen latenten Abdruck auf einem Geschirrstück hinterlassen, und ich gab ihre Fingerabdruckkarten schon mal an die Gruppe weiter, die den Verursacher desselben finden sollte. Nach und nach hatten alle die Stempelfarbe zur Fertigstellung der Fingerabdruckkarten genutzt, so dass alle tauschen konnten. Weitestgehend hatten nun alle den Ablauf begriffen, allerdings ging die Klassifizierung ziemlich unter. Ob alle auch mal durch eine der fünf Lupen geschaut hatten, und die Muster genau betrachteten, beachtete ich nicht.

Ich wollte wenigstens noch eine gemeinsame Ergebnissicherung machen, doch eine nötige Grundruhe war dafür kaum wieder herzustellen. Ich rekapitulierte an der Tafel auf Zuruf die Abläufe. Letztlich schien aber nur noch die Hälfte des Kurses dem Ganzen zu folgen. Aktiv mitschreiben sah ich nur einen. Hinsichtlich der zu schreibenden Klausur beunruhigte mich dies ein wenig. Das Übertragen der Abläufe auf das Modell des generischen biometrischen Systems fiel unter den Tisch. Die Ergebnissicherung brach in Bezug auf meine Planung eher mittendrin ab. Ich lud daher auch alle Folien und die Minutienaufgabe nochmal in das Moodle-System der Schule.

Der Kursleiter, der freundlicherweise aufmerksam hospitierte, kritisierte, dass die guten Schülerinnen unterfordert gewesen seien, und ich ruhig schneller machen könne. Gleichzeitig hätte ich zuviel für die Stunde geplant. Die Ergebnissicherung musste deutlicher herausgehoben oder als Hausaufgabe aufgegeben werden. Schneller und weniger zu machen erschien mir widersprüchlich, aber im Grunde war dies ein Hinweis auf eine fehlende Binnendifferenzierung. Das Unterrichtskonzept muss hergeben, dass sowohl Schülerinnen mit schneller Auffassungsgabe und mehr Vorkenntnissen als auch welche, die langsamer arbeiten oder noch nicht viel über ein Thema oder eine Arbeitsweise wissen, dabei bleiben. Jenseits der benannten Probleme lobte mich der Lehrer und auch ein Schüler, dass sie die Stunde spannend gefunden hätten und ihnen das Spaß gemacht habe.

Persönlich zog ich vor allem das Resümee, dass die Idee des Einstiegs über eine herkömmliche Fingerabdruckanalyse zwar spannend ist, aber noch besser zeitlich geplant

werden muss. Es muss genügend Spielraum gelassen werden für Auf-, Abbau- und Tauschphasen sowie unterschiedliche Gruppengeschwindigkeiten, was in der durchgeführten Stunde leider nicht geklappt hat. Zugleich muss durch binnendifferenzierte Aufgaben sichergestellt sein, dass auch andere weiterführende Aufgaben angegangen werden können, wenn sich jemand unterfordert fühlt.

Bericht und Resümee zum Ablauf der 3./4. Stunde Mit der Mind-Map, in der ich die Stichworte vom Brainstorming der letzten Stunde nochmal im großen Gesamtkontext einzuordnen suchte, begann ich die Stunde. So sollten die von den Schülerinnen beim letzten Mal erarbeiteten Punkte nicht untergehen. Mit Hilfe der Mind-Map stellte ich gleichzeitig vor allem die Funktionsweise, den Aufbau sowie die Fehler biometrischer Systeme erstmalig systematisch vor. Das Ganze gestaltete ich als frontales Lehrer-Schüler-Gespräch – ich fragte die teilweise vagen Vorstellungen zu den einzelnen Begriffen der Mind-Map ab, korrigierte und konkretisierte diese dann im Gespräch.

Als nächstes breitete ich in der Mitte des Konferenztisches auf unterschiedlichen Blättern gedruckte Teile eines generischen biometrischen Systems aus, um mit den Schülerinnen zusammen ein solches zu rekonstruieren. Dies war der zweite Teil der Wiederholung der letzten Stunde, gestaltet als Frage-Antwort- und Ratespiel. Die Schülerinnen zeichneten das Komponentendiagramm nicht ab, stattdessen verließen sie sich auf meine Ansage, dass ich es im Moodle hochgeladen habe.

Ich ging über zum knapp neunminütigen Werbefilm des Bundesamts für Migration und Flüchtlinge (BAMF) zum elektronischen Aufenthaltstitel (eAT) und erteilte Beobachtungsaufträge (siehe Planung, Tabelle 5.6). Der Film erregte die Gemüter – ich hatte ihn bewusst als einen Film, der ein sensibles Thema tangiert, nämlich die Verbindung von Biometrie und Rassismus, ausgewählt. Immer wieder waren schon während des Films Kommentare zu hören: „Auf der Ausländerbehörde gucken sie dich nicht mal mit dem Arsch an“, oder es wurde bei bestimmten Szenen viel gelacht (z. B. als die „Musterbeamtin“ in der Behörde die eAT-Karte hinter dem Bildschirm hochzaubert oder als sie dem „Musterausländer“ versichert, dass er keine Angst zu haben brauche, die Fingerabdruckdaten würden nur von der Polizei oder bestimmten staatlichen Behörden gelesen werden). Die Aufmerksamkeit flachte allerdings mehr und mehr ab. Daher brach ich den Film nach der Hälfte ab und fragte danach, wie sie ihn allgemein bewerten würden. Es entstand eine aufgeregte und spannende Diskussion, in der ich mich direkt an den Tisch setzte. Ich ergänzte Informationen, etwa wieviel der eAT kostet (110,- Euro), was großes Hallo ob der Ungerechtigkeit insbesondere für benachteiligte Asylbewerberinnen auslöste. Außerdem ging es um die Zustände auf den Behörden im Allgemeinen, um die Clichés des Films („das Blondchen“ oder der „Musterausländer“). Es wurde immer wieder deutlich, dass hier eine direkte Berührung zur Lebenswelt vieler Schüler bestand – die Technik wurde hier aus der Alltagserfahrung heraus greifbar.

Irgendwann lenkte ich das Gespräch auf die technischen Beobachtungsfragen und notierte die von den Schülerinnen erkannten Komponenten auf Zuruf am Whiteboard. Aufgrund des geweckten Interesses wurden jetzt konkretere Nachfragen zur Technik hinter dem eAT gestellt: Einzelne wollten z. B. wissen, wie der RFID-Chip genau funktioniere. Aber es gab auch Fragen zum Verwaltungskontext, etwa zur Gültigkeit des alten eAT (einer hatte bspw. einen unbefristeten Aufenthaltstitel und war besorgt, dass er nun auch Fingerabdrücke abgeben müsse). Um die Sichtbarkeit des RFID-Chips auf der Karte zu untersuchen, zeigte eine Schülerin ihren elektronischen Personalausweis (ePA). Sie erzählte, dass sie extra ihre Fingerabdrücke „zu ihrer Sicherheit" dort habe speichern lassen – für den ePA ist es ja freiwillig –, damit niemand anderes ihren ePA benutzen könne, aber die Online-Funktion nutze sie nicht. Leider hatte ihre Behauptung schon fast niemand mehr gehört, da sie all das sehr leise fast nur mir erzählte. Es gelang mir an dieser Stelle nicht, das Ganze in die Gruppendiskussion zurückzugeben.

Es wurde immer unruhiger. Einige beschäftigten sich mit anderen Sachen. Mitten in der Unruhe ging ich zu meinen Diskursanalyseaufgaben bezüglich Eurodac und ePass über (siehe Planung, Tabelle 5.6). Die Schülerinnen arbeiteten weitestgehend in ihren üblichen Gruppen. Eine Schülerin blieb sogar allein. Nur gut ein Drittel beschäftigte sich noch mit der Aufgabe. Eine Schülerin surfte etwa intensiv bei Facebook. Ich ging herum und versuchte mit Fragen zu motivieren – „Was findet Ihr dazu? Habt Ihr schon was?" –, aber ich war zunehmend innerlich verzweifelt. Als es endlich klingelte, war ich froh, da ich das Gefühl hatte, sie alle verloren zu haben. Ich gab die Fertigstellung der Recherche als Hausaufgabe auf und verwies darauf, dass ich auch ein Wiki angelegt habe, wo alles eingetragen werden könne.

Die Kritikpunkte des Kursleiters, der nochmal aufmerksam hospitiert hatte (in den späteren Stunden zog er sich dann komplett zurück), waren, dass ich zwar gute Impulse gegeben hatte, dann aber die Aufmerksamkeit nicht halten konnte. Noch immer unterfordere ich die guten Schülerinnen des Kurses. Ich könne ruhig schneller machen. Insgesamt sei das aber ganz gut gewesen. Ich sei manchmal zu ehrlich gewesen – man solle sich Unkenntnis nicht zu sehr anmerken lassen. Ein Beispiel war eine Bemerkung von mir beim Durchgehen der Mind-Map: „Was meinte ich eigentlich nochmal mit Nicht-Akzeptanz? Das weiß ich jetzt selbst nicht mehr…"

Der Kursleiter empfahl mir, keine Tafelbilder hochzuladen, damit sich die Schülerinnen auch selbständig Notizen machten und dabei ein gewisser Lerneffekt auftrete.

Mir kam die Stunde nicht gut gelungen vor. Insbesondere stimmte die Diskussionskultur nicht. Ein Dilemma war, dass ich einerseits sicherstellen wollte, dass die Schülerinnen die technisch definierten Begriffe und die Fakten rund um Biometrie-Systeme richtig lernen, dass sie andererseits aber eigene Ideen einbringen, den Gang des Lernens eigenständig beeinflussen und sachlich diskutieren können sollten. Ich wollte mehr in den Hintergrund treten. Bisher entstanden kaum länger anhaltende Diskussionen, in denen ich nicht eine zentrale „Ja, ist richtig, ist falsch."-Rolle gespielt hatte.

Insgesamt bestärkte sich der Eindruck, dass die Kultur eines selbständigen konzentrierten Arbeitens wenig ausgeprägt war oder sehr gut moderiert sein musste. Es war wichtig, besser zu verstehen, was die Schülerinnen an einem Thema interessiert, wie sie sich ihm nähern möchten, um nicht allzu schnell in die Rolle des Unterhalters zu verfallen. Erstaunlich ist, dass es den Kursleiter überraschte, dass ich vom restlichen Stundenverlauf enttäuscht war. Er hatte die Stunde als sehr produktiv empfunden, was für die Diskussion zum Film auch zutraf.

Lernerfolgskontrolle Klausur Die Klausur, die nach den ersten sechs Blöcken geschrieben werden musste, konzipierte ich weitestgehend entlang des bisher Erarbeiteten, sprach die Aufgaben mit dem Lehrer ab, der sie dann auch bewerten würde.[576] Die Klausur wurde von 13 Schülerinnen mitgeschrieben.[577]

Die ersten beiden Aufgaben prüften vorrangig gelerntes Wissen und dessen Einordnung in technische Zusammenhänge. Die letzte Aufgabe erforderte eine Transfer- und Anwendungsleistung des Gelernten im Rahmen einer selbständig argumentativ gestützten Beurteilung eines informatischen Systems. Sie war insofern die interessanteste, da sie für mich auch indirekt zeigte, ob und wie das im Unterricht praktisch, in den Kontroversen und in der Textarbeit gelernte Wissen in eine schriftliche Auseinandersetzung mit einem Anwendungsfall eines Fingerabdruckerkennungssystems einfloss. Um hierzu eine Einschätzung abzugeben, möchte ich im Folgenden kurz exemplarisch einige inhaltliche Ergebnisse der Klausur in Hinblick auf die Argumentationsaufgabe zusammenfassen.[578]

Die Aufgabe lautete:

> „a) Lesen Sie zunächst Anlage 2 und erklären Sie dann kurz, worum es sich bei Eurodac handelt.
> b) Nehmen Sie zu folgender Frage kritisch Stellung: *Ist der Einsatz einer biometrischen Technik wie Eurodac im Bereich der Migrationspolitik gerechtfertigt?*
> Stützen Sie Ihre Sichtweise mit aussagekräftigen Argumenten."

„Anlage 2" ist eine knappe Schilderung des Bundesverwaltungsgerichts über ein damals noch nicht abschließend entschiedenes aufenthaltsrechtliches Verfahren, bei dem es um die Frage der Mitwirkungspflicht des Asylbewerbers bei der Abgabe von verwertbaren Fingerabdrücken für das Eurodac-System ging.

Hinsichtlich des ersten Teils der Aufgabe kann ich sagen, dass die meisten ungefähr sagen konnten, worum es sich bei Eurodac konkret handelt. Es fiel auf, dass die Diskussionen im Unterricht um die Rolle einzelner Akteure nachwirkten und gezielt einige

[576] Siehe Anhang *Klausuraufgabe OSZ Handel.*

[577] Der Notenschnitt betrug 2,2 und niemand bekam eine Sechs oder eine Fünf.

[578] Direkte Zitate aus den Klausurantworten habe ich ggf. sanft in der Rechtschreibung korrigiert, den Stil, die Grammatik und Satzstellungen aber beibehalten.

benannt wurden. Außerdem fiel auf, dass technische Aspekte, Akteure, gesetzliche Bestimmungen oder der Zweck des Systems teilweise ziemlich durcheinander auf gleichen Ebenen rangierend genannt wurden – es fehlte bei vielen die Fähigkeit oder ist auch im Projekt nicht mit vollem Erfolg geschult worden, diese abstrakten Kategorien zu unterscheiden.

> „Mitwirkende der Eurodac sind die Eurokommission, Asyl-Bewerber und Drittausländer. Der Eurodac ist eine Sammelbank mit Auskünften der Bewerber und Bewerberinnen. Man benötigt den Eurodac, wenn man älter ist als 14 Jahre. Dieser dient zur Überwachung der Bewerber."

Es wird alles – teilweise falsch – „herausgegossen", was irgendwie zum Eurodac-System hängengeblieben ist. Einige Akteure erscheinen auf gleicher Ebene, der Begriff „Sammelbank" soll eigentlich „Datenbank" heißen und irgendeine rechtliche Regelung bezüglich Eurodac scheint für alle Menschen ab 14 Jahren zu gelten.

> „Eurodac ist eine Datenbank in Luxemburg und speichert Fingerabdrücke. Wurde im Jahre 2000 ins Leben gerufen.
> Richtet sich an Asylbewerber und Drittausländer. Ziel ist es zu verhindern, dass Asylbewerber in mehreren EU-Ländern Asyl beantragen. Dauer der Speicherung beträgt 2 oder 10 Jahre und [Fingerabdrücke] werden nur von Menschen ab 14 Jahren abgenommen. Hauptakteur ist die EU-Kommission."

Auch hier wird Eurodac technisch nur auf eine Datenbank beschränkt. Allerdings sind Zweck, Zielgruppe und einige rechtliche Bedingungen gut getroffen. Der Akteur EU-Kommission wird einfach nur genannt und nicht in seinem Bezug zum System erklärt – es wirkt einfach so, als ob die Antwortende meint, dass auch diese Sache mit den Akteuren vielleicht irgendwie erwähnt werden sollte.

> „Beim Eurodac handelt sich es um ein Dokument, bei dem einem die Fingerabdrücke abgenommen werden, es gibt die Identifikation eines Menschen an. Es ist aber kein ePass oder ein elektronischer Aufenthaltstitel. Hauptaktionäre sind Europäische Kommission, Honeywell, Bull.
> Kritik daran ist, dass es [Teil] unmenschliche[r] Asylpolitik [ist] und zu hohe Kosten anfallen. Eingeführt wurde der Eurodac am 11. November 2000 auf Basis des Ermächtigungsgesetzes."

Hier wird nur sehr ungefähr erinnert, was Eurodac war und sogar der historische Begriff „Ermächtigungsgesetz" unangebracht benutzt. Akteure sind zu Aktionären geworden und werden ebenfalls in keine Hierarchie oder Beziehung zu Eurodac gesetzt.

> „Bei Eurodac handelt es sich um ein EU-weites Fingerabdruckidentifizierungssystem für Asylbewerber, welches helfen soll, ihre Identität festzustellen. Das System wurde eingeführt, um den Aufenthalt einzelner Personen innerhalb der Europäischen Union

> zu überwachen und so zu verhindern, dass Personen in andere Länder abtauchen können, falls sie eine Straftat begangen haben und anderweitig nicht zu identifizieren sind. Alle Asylbewerber sind verpflichtet ihre Fingerabdrücke abzugeben, jedoch müssen diese nicht in verwertbarer Qualität sein, wie der Bayerische Verwaltungsgerichtshof zuletzt entschieden hat. Die Fingerabdrücke selber werden auch im elektronischen Aufenthaltstitel abgespeichert, welcher für Asylbewerber ähnlich wie ein Personalausweis agiert."

Diese Antwort ist nahezu perfekt und bezieht sogar direkt die für die Klausur zur Verfügung gestellten Materialien ein – es sind natürlich nicht dieselben Fingerabdrücke, die im eAT gespeichert werden, wie in Eurodac – auch hier ist noch etwas durcheinandergekommen vom im Unterricht Gelernten.

Insgesamt bilden aber die ausgewählten Antworten ungefähr das Spektrum der Qualität der Beschreibungen ab – niemand war wirklich völlig ahnungslos geblieben, aber einigen fehlte es an der Kompetenz, Gelerntes gut zu strukturieren und Zusammenhänge zwischen den wiedergegebenen Einzelfakten herzustellen und genau darauf zu achten, wonach eigentlich gefragt wird – um Akteure ging es eigentlich in diesem Falle nicht.

Der zweite Teil der Aufgabe erforderte im Grunde einen argumentierenden Aufsatz, wie er eher in den sprachlichen Fächern trainiert wird. Ich erwartete, dass in der Sekundarstufe II dieses Werkzeug schon ausreichend eingeübt ist, und hier vor allem nur noch die im Unterricht gelernten Fakten sinnvoll argumentativ gewichtet, eingeordnet und somit zur umfassenden Beurteilung eines technischen Anwendungsfalls einbezogen werden.

Grundsätzlich wurde der Einsatz des Systems in der Migrationspolitik von einigen komplett abgelehnt, von einigen teilweise und von einigen komplett befürwortet. Argumente, die fielen, waren:

- Biometrische Technik ist prinzipiell problematisch, aber im Fall der Migrationspolitik gerechtfertigt:

  > „Auch wenn ich kein Befürworter dieser Technik bin, bin ich der Meinung, dass der Einsatz im Bereich der Migrationspolitik gerechtfertigt ist, weil es bis zum heutigen Stand keine vergleichbare Alternative gibt, die in dieser Art den gewünschten Zweck erfüllt."

  > „In der Migrationspolitik ist der Einsatz von biometrischen Systemen voll und ganz gerechtfertigt, anhand dieser Identifikationsinformationen kann man ganz leicht Personen identifizieren […]"

- Der Einsatz von Biometrie ist aufgrund von Diskriminierung, Selbstverstümmelung und der immensen Kosten, die besser in eine gute Infrastruktur zur Versorgung von Asylbewerberinnen zu investieren wären, nicht gerechtfertigt.

- Der Fingerabdruck dient der Kriminalitätsbekämpfung:

„Das System hilft aber so Verbrecher abzuhalten in andere Länder abzutauchen."

„… der Fingerabdruck [ist] bei Kriminalfällen ein guter Hinweis auf einen Täter[,] was auch als handfester Beweis gilt (…) und nach Statistiken neigen auch eher Ausländer, die weniger haben als andere[,] zu Kriminaldelikten."

- Der Einsatz von Eurodac ist rechtlich unangemessen:

  „Der Fingerabdruck ist nicht zu verlangen laut Fallbeispiel."

  „Das Vorgehen von Eurodac weist mehrere negative Aspekte auf, wie zum Beispiel der fehlende Rechtsschutz oder der Datenmissbrauch von Asylbewerbern."

  „In diesem Fall ist es für den Asylbewerber besonders schwer das Gegenteil zu beweisen, ohne die Vorort sprechende Sprache zu beherrschen."

- Biometrie ist ein geeigneter Ausweisersatz:

  „Viele können sich nicht ausweisen, sprich der Passport ist nicht vorhanden und da so eins einmalig dieser Person gehört ist Eurodac eine gute, nicht beste, Alternative dafür."

- Das System funktioniert gut genug für den Zweck:

  „Durch diese Technik ist eine gewisse Richtigkeit gewährleistet und die Ordnung und Regeln werden eingehalten."

  „Ich finde zur Identifizierung einer fremden Person sind biometrische Systeme sehr geeignet, da bei Eurodac Fingerabdrücke genommen werden und sind allem Anschein nach bei jeden Menschen einzigartig."

- Ein biometrisches System lässt sich austricksen:

  „Jedoch kann man das System und Fingerabdrücke überlisten. Deswegen finde ich, dass es nicht sein darf, dass ein Bewerber deswegen nicht im Land bleiben darf."

  „Zudem kommt dazu, dass das biometrische System von Eurodac nicht einwandfrei funktioniert. Es können von der Datenerfassung bis zur Entscheidung viele Fehler auftreten (FAR)"

  „Das Problem an dieser Sache ist, es funktioniert nicht 100 % einwandfrei. In Fall des Textes handelt es sich um eine False Enrolment Rate (FER), da seine Fingerabdrücke für das System nicht verwertbar sind."

- Das System ist allgemein ungerecht:

  „[…] die meisten Menschen die Asyl beantragen haben nichts außer[,] was sie am Leibe tragen[,] und sie bei nicht verwertbaren Fingerabdrücken mit Abschiebung zu bedrohen ist das Allerletzte".

Das Meinungsspektrum zwischen Ablehnung und Befürwortung war also komplett vertreten und keine Schülerin war um Argumente, die nicht immer ganz korrekt waren und teilweise ebenfalls ein gewisses Durcheinander der gelernten Fakten zeigten, verlegen. Nur wenige waren in der Lage, das Für und Wider ausgewogen in einer logisch konsistenten Argumentationskette zu diskutieren. Die meisten wussten auf der rhetorischen Ebene eine Art Diskussion von Argumenten zu simulieren, aber führten faktisch keine durch, sondern reihten Argumente einfach ungewichtet aneinander. Der bewertende Lehrer honorierte aber schon positiv, wenn es einen Ansatz der Abwägung von Pro und Contra gab, zum Beispiel derart: „Ich finde, man kann nicht genau sagen ja oder nein. Es gibt immer positive und negative Aspekte." Hierfür setzte er die lobende Bemerkung „Gute Argumentation!" an den Textrand.

Es zeigte sich schließlich, dass das Nachbearbeiten konkreter, selbst verfasster kurzer Texte auch als Teil des Unterrichtsprojekts etwa in Form eines wohlwollenden Peer-Reviews zukünftig in Erwägung zu ziehen ist. Denn in fast allen Klausuren wurde diese Einschätzungsfrage in großen Teilen, sicherlich zum einen dem Zeitdruck einer Klausursituation, aber meiner Ansicht nach auch dem im Informatikunterricht zu wenig geübten Beurteilen von Auswirkungen einer im Alltag eingesetzten Technik geschuldet, häufig nur sehr verkürzt und implizit diskutiert.

Gesamtbilanz Die Unterrichtseinheit an der Schule war für mich vor allem eine Art Machbarkeitsstudie, ob das Gesamtkonzept prinzipiell an einer Schule durchführbar wäre. Eine systematische quantitative Evaluation etwa mit einem Fragebogen habe ich begleitend nicht vorgenommen, da ich noch umfassend mit der Verbesserung, Anpassung des Konzepts und der Vorbereitung der Stunden selbst beschäftigt war. Als qualitative Auswertung dienten mir meine Beispielberichte, das inhaltliche Feedback des Kursleiters nach den Stunden sowie seitens der Schüler in einem Zwischen- und einem Schlussfeedback (beide mündlich). Das Zwischenfeedback setzte ich spontan ein, da ich nach etwa der Hälfte der Zeit das Gefühl hatte, dass etwa die Hälfte der Schülerinnen die Lust am Thema verlor, und ich verstehen wollte, woran es lag. Danach wurde es um einiges angenehmer von der Atmosphäre her. Die Schülerinnen gaben mir sehr gute Rückmeldungen auf mein Engagement, konkret auf ihre Bedürfnisse einzugehen.

Weitere Rückmeldungen der Schülerinnen waren, dass die Unterrichtsreihe sehr informativ und durch die Gruppenarbeit und Präsentationen sehr abwechslungsreich gewesen sei und sie einiges gelernt hätten. Allerdings wurde auch gesagt, dass ich unerfahren im Unterrichten an einer Schule sei, vor allem würde ich bei Gruppenarbeiten zu lange bei einer einzelnen Gruppe helfen, sollte die Aufmerksamkeit hier besser verteilen.

Der Kurslehrer betonte zum Schluss erneut, dass er meinen Durchgang durch die Reihe zu langsam fand – interessanterweise hatte ich genau einen gegenteiligen Eindruck, vermutlich weil ich zu viele Perspektiven aufgemacht hatte. Er erwähnte noch-

mals, dass ihm einige sehr unterfordert erschienen. Meine persönliche Ausrichtung war sehr stark an den Langsameren orientiert, da ich alle „mitnehmen“ wollte. Der Lehrer des Kurses fand es zudem schade, dass ich mit dem informatischen Teil und der Software-Ebene erst gegen Ende angefangen habe. Das kam seiner Ansicht nach zu kurz und hätte an den Anfang gehört. Mir fiel auf, dass der diskursanalytische Anteil als nicht-informatisch wahrgenommen wird. Zu ausgedehnt fand der Kursleiter zudem die praktischen Teile, das Fingerabdruck-Nehmen und den Fake-Finger-Teil – das hätte exemplarisch gereicht (und vermutlich nicht für alle aufbereitet werden müssen). Bezogen auf die ganze Reihe fehlte ihm ein Spannungsbogen. Schlussendlich sah er die Unterrichtsreihe aber als Bereicherung, die aber vielleicht besser ins 3. Kurshalbjahr gepasst hätte. Er war zudem froh, die Gelegenheit für eine andere Perspektive auf die Schülerinnen bekommen zu haben. Ich denke, mit kleineren Lerneinheiten, mehr Abwechslung, das heißt auch binnendifferenzierteren Aufgaben, könnte dem Phänomen der Unterforderung sehr schneller Schülerinnen erfolgreich begegnet werden.

Die sehr positive Reaktion der Schülerinnen auf meine Einforderung eines Zwischenfeedbacks zeigte mir aber wiederum, dass es vor allem auch wichtig ist, öfter genau zu erfragen, wo die Probleme bei der jetzigen Art zu Lernen liegen, was gerade fehlt, wo es hingehen soll und so fort. Eine sehr, sehr große Herausforderung stellt das Herangehen an die Software dar. Hier ist eine gewisse Lehrroutine sicherlich hilfreich, bei der die Lehrende das selbständige erforschende Lernen und Fehlerfinden motiviert.

Mir wurde auf mehreren Ebenen klar, dass mein Lehr- und Lernmodul noch sehr überarbeitungsbedürftig ist:

Erstens bedürfen insbesondere die Gruppenarbeiten und die materialintensiven Phasen einer maßgeschneiderten Planung und ruhigen Durchführung. Es sollte alles Nötige vorhanden und vorher einmal ausprobiert worden sein. Innerhalb gestellter Aufgaben muss es eine Bandbreite an Schwierigkeitsgraden geben, so dass keine Unterforderung auftritt. Auch sollte gegenseitige Unterstützung stärker aktiv eingeplant werden. Der didaktische Ansatz des Gruppenpuzzles[579] eignet sich hierfür insgesamt hervorragend und könnte auf alle Gruppenarbeiten übertragen werden.

Zweitens sollte die Moderation von Gruppendiskussionen sehr gut vorbereitet sein, damit sie nicht so schnell im Sande verlaufen oder in Allgemeinplätzen versanden. Dazu gehört das aussagenbezogene, genauere Erfragen von Begründungen, Bitte um das Herstellen von Bezügen und das Geben von Beispielen. Außerdem muss ein zu stark auf die Lehrerin fixiertes Diskutieren durch geschicktes Zurückgeben von Fragen in die Gruppe, das Herstellen von Bezügen zwischen den Aussagen verschiedener Beteiligter, aber auch das Reflektieren und Wiederholen von einzelnen Argumenten befördert werden. Die Diskussionskultur selbst könnte als gemeinsam reflektierte Methode behandelt werden und die Moderation der Diskussionen nach und nach an

[579] Zur Methode des Gruppenpuzzles (*Jigsaw Teaching Method*) vgl. Aronson und Patnoe 1997 und die Webseite zur Methode https://www.jigsaw.org, letzter Abruf 30.7.2017.

Kursteilnehmerinnen abgegeben werden. Auch Methoden des sogenannten Schreibdenkens könnten für die Leiseren hier Möglichkeiten der Beteiligung bieten.[580]

Drittens ist insbesondere der software-analytische Teil noch zu unkonkret und führt schnell zu Frustration, wenn hier pauschal Code-Schnipsel mit ungewohnten Tools bearbeitet werden. Hier treten schnell typische Informatik-Lehrerinnen-Fallen auf, wie zu lange Fehlersuche mit Einzelnen, die gemieden werden sollten.[581]

Mit Blick auf die Klausur, die leider jenseits einer mündlichen Feedbackrunde, meine einzige konkrete, greifbare Rückmeldung darstellt, kann ich viertens feststellen, dass zum einen keine der mitschreibenden Schülerinnen wirklich verstanden hat, was Eurodac eigentlich genau ist, also, auch die Rechercheaufgabe im Unterricht nicht nachhaltig Klärung darüber gebracht hat. Zum anderen bestehen größere Defizite, Urteile und Einschätzungen zu den Auswirkungen einer Überwachungstechnologie in der Gesellschaft logisch schlüssig zu argumentieren. Argumentieren ist sicherlich eine Fähigkeit, die in allen Unterrichtsfächern geübt werden sollte, aber sie besitzt in jedem Fachgebiet eine spezielle Ausprägung. Bereits in den Bildungsstandards der Gesellschaft für Informatik e. V. für die Sekundarstufe 1 heißt es für den Prozesskompetenzbereich *Begründen & Bewerten*:

> „Schülerinnen und Schüler der Jahrgangsstufen 8 bis 10
>
> - formulieren angemessene Bewertungskriterien und wenden diese an,
> - gewichten verschiedene Kriterien und bewerten deren Brauchbarkeit für das eigene Handeln,
> - wenden Kriterien zur Auswahl von Informatiksystemen für die Problemlösung an und bewerten diese.
>
> In diesen Jahrgangsstufen entwickeln die Schülerinnen und Schüler auch eigene Kriterien und Maßstäbe zur Bewertung informatischer Sachverhalte. Sie vertreten argumentativ ihren Standpunkt, setzen sich kritisch mit den Argumenten anderer auseinander, sodass sie ihre Verantwortung bei der Nutzung von Informatiksystemen wahrnehmen können.“[582]

Die Mini-Aufsätze in den Klausuren zur Beurteilung von Eurodac anhand eines Fallbeispiels haben gezeigt, dass hier Nachholbedarf besteht. Es werden viele Phrasen des hegemonialen Diskurses übernommen, Befindlichkeiten nicht klar von Fakten getrennt und logische Schlüsse unvollständig ausgeführt. Viele Teilschritte in den Gedankengängen werden gar nicht ausformuliert. Hier zeigt sich, dass die grundlegend diskursanalytische Herangehensweise mit einem Fokus auf der Analyse von

[580] Siehe Scheuermann 2013.

[581] Auch hier gibt es schöne Methoden, dies zu vermeiden, etwa die Support-Warteschlange, einen Live-Chat, Fehler-Meetings, FAQs, vgl. Hartmann, Näf und Reichert 2007, S. 151.

[582] Brinda u. a. 2008, S. 20.

Argumentationsweisen verschiedener Akteure viel stärker ausgeprägt werden muss, vielleicht auch einzige intensiv geübte Methode einer solchen Reihe sein sollte. Die Notwendigkeit eines solchen Vorgehens kommt auch darin zum Ausdruck, dass die Auseinandersetzung mit politischen und gesellschaftlichen Dimensionen gerade auch vom Kurslehrer als nicht-informatischer Teil und daher als eher beiläufig interessant wahrgenommen wurde.

Insgesamt sehr positiv zu bewerten und beizubehalten sind die taktilen praktischen Elemente wie das Ausprobieren der analogen Fingerabdruckabnahme und händische Lesen und Vergleichen der Muster – dies war ein sehr anschaulicher Einstieg für die meisten. Sehr hilfreich, um das Interesse der Schülerinnen an der Technik zu wecken, waren tatsächlich direkte Berührungspunkte zum lebensweltlichen Alltag – wie im Fall der Erfahrungen bei Behörden. Hier entstand aus persönlicher Betroffenheit schnell ganz bewusstes Interesse daran, wie die involvierte Technik genau funktioniert. Auch der Methodenmix sowie der prinzipielle Theorie-Praxis-Transfer zwischen experimentellen Phasen und reflektierenden Lese-, Diskussions- und Vortragsphasen hat sich meines Erachtens bewährt, kann nur insbesondere bei der Arbeit mit Software noch methodisch verbessert werden.

5.3.3 Universitätsseminar am Institut für Informatik, HU Berlin, 2012/13

Eine weitere gute Gelegenheit, das Konzept der Lerneinheit zu verbessern, bot sich im Rahmen meiner eigenen Lehre als wissenschaftliche Mitarbeiterin am Institut für Informatik.[583]

Lern- und Lehrvoraussetzungen

Das Seminar »Automatisierte Fingerabdruckidentifizierung praktisch hinterfragen« konnte im Rahmen des Diplom-Hauptstudiums oder Masterstudiums Informatik aus einer breiten Themenpalette im Gebiet der Praktischen Informatik zu belegender Wahlpflichtangebote im Wintersemester 2012/13 ausgewählt werden.

Das Seminar wurde in dem zu unserer Arbeitsgruppe »Informatik in Bildung und Gesellschaft« gehörenden kleinen Tagungsraum abgehalten, in dem ca. 15 bis 20 Teilnehmende maximal Platz fanden. Die Tische und Stühle waren u-förmig einander zugewandt angeordnet. In der Regel wurden im Seminar durch die Studierenden keine Laptops genutzt, höchstens zur Protokollierung. Für die Dozentin gab es ein Whiteboard und einen Beamer für die Präsentation. Mein Büro war nur wenige Räume von dem Seminarraum entfernt. Ich hatte selbst einen Schlüssel für den Seminarraum und konnte relativ problemlos auf diverse Ressourcen (fehlende Kabel, Scanner, Drucker, Adapter, Laptops, Stifte, Papier…) zurückgreifen.

[583] http://waste.informatik.hu-berlin.de/Lehre/ws1213/SE_FingerIdent, letzter Abruf: 30.7.2017.

Insgesamt nahmen 13 Studierende über die gesamte Kursdauer teil, drei davon weiblich. Drei Studierende kamen extra von der Technischen Universität Berlin, da sie das Thema spannend fanden. In Bezug auf die kulturelle Prägung war der Kurs eher homogen Weiß und deutsch, wobei ich das nicht explizit erfragt habe, sondern auch hier nur vorurteilsbehaftete Schlüsse aus den Namen, dem Äußeren und dem allgemeinen Verhalten und Äußerungen ziehe. Vom disziplinären Hintergrund her waren zwei Soziologie-, Techniksoziologie- und sonst Informatikstudierende dabei, die meisten hiervon im Informatik-Masterstudium, eine Person für das Lehramt sowie zwei im Diplom-Informatik-Hauptstudium. Die informatischen Vorkenntnisse waren nicht zuletzt deswegen etwas unterschiedlich. Zwei, drei Leute hatten zudem bereits vertiefte Vorkenntnisse in Signalverarbeitung und Security Engineering.
Insgesamt kann von Studierenden in dieser späten Phase des Studiums ein hohes Maß an Eigenständigkeit erwartet werden. Das heißt, sie sind es gewohnt (oder sollten es zumindest gewohnt sein), selbständig Texte zu recherchieren, zu lesen und auszuwerten, das Wesentliche daraus themengebunden in Vorträgen zu präsentieren und aktiv einen Seminarverlauf mitzugestalten, zu diskutieren sowie auch wissenschaftliche Texte zu verfassen. Insbesondere letzteres kommt allerdings im Informatik-Studium jenseits von Bachelor- und Masterarbeit deutlich zu kurz.

Seminarplanung

Das Seminar bestand aus 16 Einzelterminen sowie einem zusätzlichen optionalen Termin für die Vorbereitung des für den Schluss geplanten Überwindungstests. Die ersten beiden Drittel aller Sitzungen bestanden aus Vorträgen zu den in meiner Einführung vorgestellten Themenbereichen mit selbstständig zu erarbeitenden Schwerpunkten (ggf. Bereitstellung von Materialien meinerseits) und anschließenden Diskussionen dazu, in die ich neben den Referentinnen moderierend eingriff.
Themen:

- Manipulationstests optischer Fingerabdruckscanner,
- Fake-Fingerprint-Detection – Lebenderkennung,
- Rekapitulation, Erweiterung und Systematisierung technischer Fehler biometrischer Systeme,
- Untersuchung kommerzieller Biometrie-Software und ihrer Visualisierungen,
- Was wird in öfftl. Performanztests wie dem FVC getestet?,
- Fallbeispiel: Aadhaar,
- Analyse und Vorstellung eines Open-Source-Fingerabdruckidentifizierungssystems: SourceAFIS,

- Quiz AFISITY zur Festigung zentraler biometrischer Grundbegriffe.

Im letzten Drittel sollten schließlich kleine „Mini-Diskursanalysen“ als Essays von etwa fünf Seiten Länge verfasst werden – die Aufgabenstellung hierfür lautete wie folgt:

> „Sucht Euch ein *biometrisches System*, das in einen *konkreten Anwendungskontext* integriert ist, und *sammelt Zeitungsartikel* dazu. Schaut Euch die *Komponenten des Systems* selbst genauer an und wählt *drei Akteursgruppen* rund um das System aus, deren *Beziehung*, *Interessen* und *Einflussmöglichkeiten* im Gesamtsystem Ihr näher *anhand ihrer Äußerungen* betrachtet.“

Die Essays sollten dann jeweils über mehrere Termine verteilt von allen gemeinsam gelesen und ausgewertet werden, um ein Feedback auch zum gelungenen Verfassen eines kurzen Sachtextes in weiterer Schulung wissenschaftlichen Schreibens zu bekommen.

Außerdem versuchte ich diesmal die Studierenden aktiv in die Planung der praktischen Tests einzubinden, da mir aus den bisherigen Erfahrungen klar war, dass hier die meisten frustrierenden Erlebnisse entstehen können und gute „Bastelstunden“ nur mit dem Einbringen der kreativen Ideen und der Aufmerksamkeit aller gelingen.

Bericht und Reflexion der Durchführung

Ein ganz besonderer Erfolg des praktischen Teils war, dass wir erfolgreich den U.Are.U-Fingerabdruckscanner überlisten konnten und zwar mit verschiedenen Fingern. Es erwies sich als sehr hilfreich, die Studierenden sowohl in die konkrete Ablaufplanung des Experiments als auch teilweise in die Beschaffung der Materialien einzubinden. Zudem profitierte ich von meinen Erfahrungen in Bremen und in der Schule und konnte ganz spezielle Problembereiche, die viel Zeit gekostet hatten (Sichtbarmachung eines latenten Abdrucks, Bildbearbeitung), ganz gezielt als problematisch genau vorbesprechen. Eine gute Entscheidung war, einen extra Vorbereitungstermin für die praktischen Experimente zu machen, um zu vermeiden, sich zu lange an organisatorischen Fragen und Aufbauproblemen aufzuhalten. Drei der Studierenden waren hochmotiviert und hatten viele sehr gute Ideen, Geduld und Fingerfertigkeit. Sie kamen zum Beispiel auch darauf, dass sich mit einer hochauflösenden Kamera der Finger eigentlich auch bereits direkt abfotografieren ließe.[584] Außerdem war mit Hilfe von Tesafilm ein latenter Fingerabdruck sehr gut zu konservieren. Zwei hervorragende Studierende hatten bereits im Rahmen ihres Vortrags selbst viel mit Gelatine herumprobiert – in Teilen auch erfolgreich – und auch versucht, einen nicht gut dokumentierten Fingerabdruckscanner für das Arduino-Board lauffähig zu bekommen.[585]

[584] Ende 2014 haben diese Idee dann auch medienwirksam Hacker des CCC umgesetzt, vgl. Krempl 2014.

[585] Siehe Vortragsfolien Schmelzer und Steinfeldt 2012.

Die Begeisterung der Studierenden hat mich selbst mitgerissen und gezeigt, dass sich ein solches Praxis-Experimentier-Seminar, bei dem viele Ausgangsvariablen eher vage sind und das „Hacking" auch komplett scheitern kann, doch lohnt. Es hat hier genauso funktioniert, wie ich es erhofft hatte: Dass der Wille zur Dekonstruktion, zum Austricksen, zum Finden der Schwachstelle genügend Neugier bietet, sich mit einem informatischen System eingehender zu beschäftigen und angstfrei vieles damit auszuprobieren. Zudem war durch die Vorträge und Essays eine politische und ethische Ebene der Auseinandersetzung gegeben, bei der die technische Spielerei im Lichte verschiedener Anwendungen, aber auch ihrer theoretischen Voraussetzungen betrachtet werden konnte. Es gab viele Diskussionen um das Für und Wider des gesellschaftlichen Sinns und Wirkens einer biometrischen Technik, um ihre Implikationen und das daran gebundene Menschenbild. Hochinteressant war auch die kritische Auswertung der Ergebnisse des *Fingerprint Verification Competition*, der letztlich als für große hoheitliche Überwachungsanwendungen nicht aussagekräftig eingeschätzt wurde.[586] Die Beschäftigung mit den systeminhärenten Fehlern zeigte sich insgesamt aber selbst für bereits fast fertig ausgebildete Informatikerinnen als kompliziertes Themenfeld.

Auch die Essays waren qualitativ sehr verschieden. Viele Argumentationsdefizite, die es auch bei den Schülerinnen gab, besonders hinsichtlich der klaren Ausformulierung eigener Gedankengänge in Form von nachvollziehbaren Zwischenschritten, wie die Autorinnen zu bestimmten Bewertungen und Urteilen kommen, waren auch in den studentischen Essays zu verzeichnen. Das gemeinsame Ausdiskutieren der einzelnen Texte konkret bezogen auf Struktur und Konsistenz der Texte war hier sehr aufschlussreich.

In der Gesamtrückschau war das Seminar gelungen konzipiert. Insbesondere die Angebote von fakultativen Extra-Terminen und die Einbindung der Studierenden in die infrastrukturelle Vorbereitung der Experimente (auch per Mail und Wiki) war eine gute organisatorische Entscheidung, um die unangenehmen „Momente des Scheiterns" durch irgendein vergessenes Material, einen unpassenden, unvorhergesehenen *Workflow* zu einem besseren Lernmoment für alle Beteiligten zu machen. Hier passte allerdings auch die Langfristigkeit eines über ein Semester gestreckten Workshops mit Wochenpausen zwischen jeder Sitzung. Ein ebenfalls gelungenes Konzept war die Rückmeldung zu den diskursanalytischen Essays der Studierenden in gemeinsamen Sitzungen. Die direkte Arbeit an stilistischen und inhaltlichen Problemen eines Texts in der Diskussion recht unterschiedlicher Einschätzungen anderer, die die gleiche Aufgabe hatten, zeigte sich als sehr produktiv, ließ die geleistete Schreibarbeit nicht untergehen und ermöglichte unmittelbare Rückmeldung zu handwerklichen Aspekten des Schreibens und Argumentierens. Zugleich wurden wiederum detaillierte technische Aspekte zu konkreten biometrischen Anwendungsfällen diskutiert und präzisiert.

[586] Siehe auch Diskussionsprotokoll hierzu unter http://waste.informatik.hu-berlin.de/Lehre/ws1213/SE_FingerIdent/29112012/protokoll_291112.html, letzter Abruf: 30.7.2017.

5.3.4 Fazit: Ein interdisziplinäres Lern- und Lehrkonzept Biometrie

Auf alle durchgeführten Umsetzungen des im Werden befindlichen Lernkonzepts zurückblickend war das Universitätsseminar das erfolgreichste, da es eine Annäherung an das Thema auf fast allen anfänglich geplanten Ebenen in ausreichender Tiefe ermöglichte und viele Studierende sich aktiv in die Entwicklung und Umsetzung der Seminaridee und der -planung einbrachten.

Die größte Herausforderung stellte dagegen die Umsetzung als Unterrichtsreihe am OSZ Handel 1 dar. Es war besonderes herausfordernd, die Schüler zu motivieren. Ihre Aufmerksamkeitsspannen waren geringer als die der Studierenden, was sich sowohl bei Lektüre als auch beim Arbeiten am Quellcode als schwierig erwies. Auch die Lernvoraussetzungen, die schon ausgeprägten Inhalts- und Prozesskompetenzen variierten im schulischen Kontext viel stärker, da noch keine starke Spezialisierung stattgefunden hat.

Ein Lernkonzept, dass sowohl den schulischen als auch den universitären Anforderungen gerecht wird, muss in seinen Anforderungen und Umfängen vielfältig skalierbare, also stark differenzierte Module bieten. Eine Anpassung dahingehend steht noch aus.

In seiner bisherigen Form kann der bildungstheoretische Ansatz der gesamten Reihe als Versuch der Zusammenführung wichtiger Bausteine einer überwachungskritischen Informatikbildung gesehen werden.

Ein Fingerabdrucksystem wird hierbei zu einem System, an dem man lernt – konkreter: an dessen Fehlern man lernt. Die praktischen Anteile ließen sich noch viel besser in einem Lern-Fingerabdruckerkennungssystem (im Sinne eines *Tangible Interface*) abbilden, wie es Schelhowe vorschlägt.[587] Denn gerade hier liegt eine „kritische Anwendung“ vor, deren Entscheidungen von gravierender Relevanz für die persönliche Lebensführung sein können:

> „Dazu müssen die Systeme transparent sein, Aufschluss über ihre Operationen geben. Dies kann einerseits durch Schulung und Ausbildung erreicht werden, wie es gegenwärtig weitgehend der Fall ist. Dies muss aber auch mehr und mehr als Anforderung an das Design solcher Systeme gestellt werden: Die Potenziale des Mediums selbst können genutzt werden, damit Verstehen und sinnliche Erfahrung zusammenwirken können.“[588]

Sich mit den Fehlern eines Biometrie-Systems zu beschäftigen, impliziert allerdings nicht zwangsläufig eine gelingende Fehlerkultur. Dazu gehören auch Anpassungen in den Lehrpraktiken: In der Informatikdidaktik für die Schule gibt es beispielsweise die Empfehlung, ein Bewusstsein für die Alltäglichkeit von Fehlern zu schaffen und einen systematischen Umgang mit Fehlern und Strategien der Fehlersuche und -behebung

[587] Schelhowe 2012, S. 269 f.

[588] Ebd., S. 270.

zu lehren – ein klassischer Fehler sei hier ein zu frühes Helfen und Selbstlösen durch die Lehrerin, um Zeit zu sparen.[589] Hier lässt sich ganz einfach etwas verändern, wenn man den Fehlern die nötige Zeit gibt.

Die Umsetzung eines geduldigen Fehlerbearbeitens ist in der Schul- oder Hochschuldidaktik angesichts struktureller Beschränkungen insofern manchmal schwierig, als dass beispielsweise Zeitdruck, eindimensionale Quantifizierung von Kompetenzen in einer einzigen fachlichen Endnote, Überforderung der Lehrkräfte durch zu hohe Lehrbelastung, mangelnde didaktische Ausbildung von Hochschullehrerinnen genau das gegenteilige Verhalten befördern. Anders sieht es in Bereichen informeller, außerschulischer, -universitärer Bildung sowie in betrieblichen Ansätzen für eine Fehlerkultur aus.

Abschließend sei noch zusammengefasst, welche Elemente sich in allen drei Settings, mit Verbesserungen über die Zeit, bewährt haben:

- praktisches Überlisten eines Fingerabdruckerkennungssystems,
- diskursanalytische Kontextualisierung,
- Codeanalyse – hier besteht allerdings weiterhin handwerklicher Verbesserungsbedarf,

Alle drei Ebenen können und müssen in unterschiedlichen Graden an Komplexität und Eigenständigkeit konzeptioniert werden, um einzelne Aufgabeneinheiten flexibel und den Lernvoraussetzungen gerecht werdend kombinieren zu können. Des Weiteren sind alle drei Ebenen wichtig in Bezug auf die verschiedenen Fehlerkategorien (Überwindungsfehler, Fehler gesellschaftlicher Einbettung, Systemfehler). Sie sind ebenso notwendig, um den angestrebten Kompetenzerwerb in den Bereichen des Begründens und Bewertens, Darstellens und Interpretierens, Kommunizierens und Kooperierens sowie Stukturierens und Vernetzens (vor allem diskursanalytischer Teil) sowie des Modellierens und Implementierens (die beiden anderen Elemente) abzudecken.

[589] Hartmann, Näf und Reichert 2007, S. 156 ff.

6 Schluss

Diese Arbeit hatte zwei Ziele:

(1) die Analyse und Systematisierung der verschiedenen Darstellungen der Fehler und Probleme biometrischer Fingerabdruckerkennungstechnologien und deren Implikationen, Verflechtungen und Wirkungen,

(2) darauf aufbauend die Entwicklung eines Lehr- und Lernkonzepts für eine kritische Vermittlung der Fehler und Probleme von Fingerabdruckerkennungssystemen.

Das erste Ziel spitzte sich mit dem Rückgriff auf die diskursanalytische Herangehensweise auf zwei Fragen zu: Wie gestaltet sich der Fehlerdiskurs in der Forschung zur Fingerabdruckerkennung, was zeichnet ihn aus? Das zweite auf die Frage: Wie könnte man eine solche kontext-/diskursanalytische Herangehensweise sinnvoll in ein biometrie-kritisches Lernkonzept zu den Fehlern einbinden? Diese Fragen sollen im Folgenden beantwortet werden.

Wie gestaltet sich der Fehlerdiskurs in der Forschung zur Fingerabdruckerkennung, was zeichnet ihn aus?

Die Systematisierung der biometrischen Fehlerforschung wurde anhand eines breit gefassten Fehlerbegriffs vorgenommen, der eine Dysfunktionalität des Fingerabdrucksystems hinsichtlich seiner Anforderungen bedeutet. In der Arbeit wurden hierfür fünf verschiedene Fehlergruppen gewählt:

A QUANTIFIZIERTE UND STARK FORMALISIERTE FEHLER – umfassen Performanz- und hier nicht vertieft betrachtete Konformanzfehler (letztere in Bezug auf Standardisierung),

B FEHLER DURCH DYNAMIK VON KÖRPER UND UMGEBUNG – umfassen Fehler, die dadurch entstehen, dass die Technik nicht ausreichend auf sich ändernde Umwelt- und Körperbedingungen angepasst ist,

C ÜBERWINDUNGSFEHLER UND STÖRANFÄLLIGKEIT – umfassen gängige Fehlerkategorien der IT-Sicherheit,

D BEGRIFFS- UND ERKENNTNISTHEORETISCHE FEHLER – umfassen Verkürzungen oder Umdeutungen der Technik zugrundeliegender Begriffskonzepte, die zu Fehlern der Deutung ihrer Funktionalität führen,

E FEHLER IM GESELLSCHAFTLICHEN KONTEXT – umfassen Fehler, die vor allem andere Disziplinen als problematische gesellschaftliche Auswirkungen oder unangebrachte gesellschaftliche Nutzung der Fingerabdruckbiometrie benennen.

Mit Hilfe dieser Systematik wurde der übliche Blick der Informatik auf Biometrie-Fehler als System-, Anpassungs- oder Überwindungsfehler (A-C) um zwei Gruppen erweitert, die auch im Verantwortungsbereich der Informatik liegen: Die eine betrifft falsch oder zu wenig in ihrer Vieldeutigkeit verstandene Begriffe, die zu Problemen in der Deutung von Anforderungen an Fingerabdruckerkennungssysteme oder falschen Grundannahmen darüber, welchem Zweck sie dienen, führen (D). Die andere betrifft ausgeblendete Analysen der gesellschaftlichen Implikationen und Auswirkungen der Fingerabdrucksysteme (E). Aber auch die zweite Kategorie (B) ist ein in der Regel eher randständig bearbeitetes Gebiet der Gebrauchstauglichkeitsforschung. Die Kategorien steigen in ihrer Komplexität an, enthalten einander. Bezogen auf Weingardts Fehler-Rahmentheorie sind A-C das disziplinäre Fehlerfeld, D ist die Rückkopplungsebene in den im Rahmen meiner Arbeit als Fehlerdiskurs bezeichneten Kontext.

Inwiefern und dass sich alle diese Kategorien überlagern, aber gerade auch die Begriffsverständnisse zentral sind, wurde zum einen an der Herleitung der Systematisierung aus dem Systemdesign deutlich gemacht. Es wurde aber zum anderen ganz besonders in der Betrachtung der als Grundannahmen für das Funktionieren der biometrischen Fingerabdruckerkennung betrachteten Kategorien Eindeutigkeit, Permanenz und Universalität einer Charakteristik in der Diskursuntersuchung deutlich. Die korrekte Modellierung insbesondere der Eindeutigkeit ist von großer Bedeutsamkeit für die Performanz des Systems. Der Begriff wird in dieser Modellierung ein anderer, klar operationalisierbarer. Die wahrscheinlichkeitstheoretische Interpretation der Eindeutigkeit lässt sich aber nicht in einem Sicherheitsdiskurs vermitteln, in dem es um verlässliche Entscheidungen der Technik geht. Auch Permanenz und Universalität haben sich als eine Frage der Auslegung von Körperlichkeit gezeigt. Ebenso stehen alle drei Begriffe zur Disposition, wenn beispielsweise mit einem Systemhack der ganze Sinn des Systems unterlaufen wird. Der Verweis auf die Akteure, die sich im Diskurs um biometrische Systeme vernetzen, sollte zudem zeigen, dass eine strikte Trennung von Informatik und „den anderen“ nicht möglich ist, da es sich um politische Systeme handelt, die verkauft werden, und hierbei wird immer auch mit Begriffen gehandelt, die im Rahmen ihrer Formalisierung auf Ebenen abstrahiert werden, die sie im politischen Diskurs nicht sind.

Es ist bereits schwierig, den Begriff *Fingerabdruckerkennung* als gut geeignet für das anzusehen, was er meint. Diese Feststellung zielt weniger darauf ab, dass die Rede vom „Abdruck“ heute in vielen Anwendungsszenarien nicht mehr zutrifft. Wenngleich auch das sicher richtig ist: Die Art der Repräsentationen der Hautleisten einer Fingerkuppe sind sehr vielfältig – vom Grauwertrasterbild, über Frequenzspektren, Merkmalsvekto-

ren hin zu Modellfunktionen. Auch die Bilderfassung ist auf zahlreiche Arten möglich, bei denen kein Abdruck mehr mit Tinte auf Papier angefertigt wird. Dennoch ist der Begriff *Finger**print*** so fest etabliert (ähnlich wie beim Verhältnis traditioneller Buchdruckverfahren zum 3D-Druck), dass dem Wort „Druck" seit seiner Digitalisierung die erweiterte Bedeutung „Abbilderzeugung auf beliebige Weise" zukommt.

Ein viel größeres semantisches Problem ist aber, dass *Fingerprint* zudem *die* Metapher für Einzigartigkeit schlechthin ist. Trotz aller „rein technischen" oder „rein mathematischen" Modelle und Definitionen, die abstrakte Kriterien für die relative Eindeutigkeit des Fingerabdrucks festsetzen, ist genau die alltägliche Metapher die Anforderung an das Produkt Biometrie. Fingerabdruckerkennung meint nämlich nicht nur das automatisierte Vergleichen von auf verschiedene Weise angefertigten und mehrfach transformierten digitalen Abbildern von Fingerkuppen oder von latenten Fingerabdrücken, sondern eben auch die daraufhin erfolgende automatische Zuordnung zu einer auf eine Person bezogenen Referenz. Doch die letztere Bedeutung war auch vor der Automatisierung stets nur implizit im Wort Daktyloskopie oder auch Fingerabdruckerkennung/-identifizierung enthalten, obwohl gerade die Personenwiedererkennung doch der eigentliche Zweck des ganzen Aktes ist. Die Person wird erst durch den Fingerabdruck technisch eindeutig-universell-permanent. Für diese Eigenschaften wird der Begriff synonym auch verwendet. In der Kryptografie gibt es *Fingerprints*, die die Authentizität eines Schlüssels bezeugen sollen. Dasselbe Prinzip wird in der digitalen Dokumenterstellung und -archivierung genutzt. Von *Browser-Fingerprinting* ist die Rede, wenn Menschen anhand ihres Surfverhaltens identifiziert werden. Die DNA gilt als „genetischer Fingerabdruck". Letztlich ist Fingerabdruckerkennung sogar auch das Sinnbild für die restliche Biometrie:

> „In fact, fingerprint-based biometric systems are so popular that they have almost become the synonym for biometric systems."[590]

Doch lässt sich mit den herausgearbeiteten Problemen der verschiedenen semantischen Ebenen einiger Grundbegriffe der Biometrie und ihrer Funktion innerhalb eines Sicherheitsdiskurses auch die eingangs der Analyse vorangestellte Arbeitshypothese stützen, dass ein gutes Funktionieren der Systeme zweitrangig für ihre allgemeine gesellschaftliche Durchsetzung ist, da die Bedrohung des „Identitätsbetrugs", der Glaube an die Messbarkeit von Identität und die wirtschaftliche Wachstumsdynamik von biometrischen Systemen viel bedeutsamer sind?

Es konnte herausgestellt werden, dass im fachlichen Diskurs eine umfangreiche und vor allem produktive Auseinandersetzung mit den Fehlern biometrischer Systeme stattfindet. Regelmäßig werden neue, gut geförderte und breit angelegte Kooperationsprojekte zwischen Staat, Wissenschaft und Industrie gegründet, die sich um Aufklärung über Biometrietechnik bemühen und auch für umfangreiche operationale Tests

[590] Maltoni u. a. 2009, S. 34.

der Technik werben, um den keinesfalls geleugneten, aber stark anwendungsbedingten Fehlern besser begegnen zu können. Ein wichtiges Ziel der Aufklärung ist die Milderung von in der Bevölkerung konstatierten Ängsten vor einer überbordenden Überwachung mit Hilfe biometrischer Technik. Unabhängig davon ist neben weitestgehend erfolglosen Klagen kein Einbruch des Absatzmarktes für Fingerabdruckerkennungssysteme festzustellen – eher im Gegenteil. Gerade die hoheitlich großflächig implementierten Systeme in Europa konnten auch zu allererst nach der Kriminaltechnik vor allem an Punkten eingesetzt werden, an denen es nur wenig Gegenwehr geben kann, da die Usees stark unterlegen sind: im Bereich der unerwünschten, illegalisierten Einwanderung und in der Asylpolitik. Hier begann die Ausweitung des Einsatzes biometrischer Systeme bereits vor „9/11".

Wie in der Auswertung der Diskursbetrachtung ebenfalls festgestellt wurde, sind sie fester Bestandteil eines Sicherheitsdiskurses, in dem biometrische Techniken vor einer schwer zu fassenden Angst vor anonymer Kriminalität schützen sollen und eine symbolische Politik stützen, in der wenigstens *etwas* dagegen getan wird.

Es konnte ebenso gezeigt werden, dass es zwar durchaus eine begriffliche Sensibilität für das Nichtzueinanderpassen von dem in der Biometrie definierten Identitätsbegriff zu dem der Personenidentität gibt. Aber letztlich gibt es keine ernsthaften Versuche, einer Überinterpretation der Fingerabdruckerkennung als Identitätsfeststellung und damit auch der Essentialisierung der Person anhand ihrer biologischen Charakteristika entgegenzuwirken. Die Reduktion einer Personenidentität auf die reine Wiedererkennung von Personenmerkmalen entkoppelt einen Menschen von den aktuellen Umständen seines Handelns, determiniert seine Möglichkeiten. Das ist einerseits genau ihr Zweck, andererseits aber auch genau das Problem. Die Entscheidung über einen Zugang zu einer Ressource wird lediglich an Daten geknüpft, deren automatisierte Prüfung und Prüfungsfehler mit der Maschine nicht verhandelbar sind. Aus diesem Grund sollte ein Fingerabdruck in einem Prozess auch nicht mehr als ein Indiz sein – erst im Kontext einer umfassenden an viele Beweise geknüpften Tatkonstruktion entsteht eine nachvollziehbare und be- oder verurteilbare Handlung. Doch gern wird im Zusammenhang mit Fingerbiometrie immer mal an die alte Fantasie einer automatisierten Beweisführung, wie sie einige Kriminalbeamte hatten und haben, erinnert.

Die genannten Teilergebnisse der Analyse bieten gute Anhaltspunkte, dass die These Bestand hat und sich vertiefte Untersuchungen des Identitäts- und des Sicherheitsbegriffs in der Informatik lohnen, um besser zu verstehen, wie ihre impliziten Bedeutungen zum Motor des in die Technikentwicklung hineingetragenen Sinns werden, ohne dass er nochmal speziell hinterfragt wird.

In der gegenwärtigen politischen und wirtschaftlichen Lage funktioniert die Fingerabdruckidentifizierung gut genug, als dass *False Positives* oder Spezialbehandlungen von Menschen, die nicht in die Vermessbarkeit der hoheitlichen Anwendungen hineinpassen, in Kauf genommen werden. Die biometrischen Techniken vertiefen die Idee und

den Sinn des Ausweispapiers und die einfache Verwaltbarkeit der Person als Datenansammlung. Sie sind so dynamisch wie die Identität, die sie manifestieren sollen.

Schließlich wurde im zweiten Teil der Arbeit versucht, die Überlegungen in ein Lehr- und Lernprojekt einfließen zu lassen, das sich Fingerabdruckerkennungssystemen über ihre Fehler annähert – die handlungsleitende Frage war dabei:

Wie könnte man eine solche kontext-/diskursanalytische Herangehensweise sinnvoll in ein biometrie-kritisches Lernkonzept zu den Fehlern einbinden?

Im Rahmen der Arbeit wurden mehrfach Lehrveranstaltungen zum Thema der Fehler von Fingerabdruckerkennungssystemen mit Rückgriff auf diskursanalytische Methodik und Methoden des Hands-On-Lernens durchgeführt und konzeptuell weiterentwickelt. Die gleichzeitige Umsetzung einer diskursanalytischen UND praxiorientierten Lehre anhand des genannten Themas war eine unterschätzte Herausforderung. Es hat sich insgesamt gezeigt, dass eine prinzipiell kritische, dekonstruktivistische Herangehensweise an die Technik und die sie begleitenden medialen Diskurse, das Befragen der Formulierungen der Akteure etwas in der Informatik Ungewöhnliches, Ungeübtes und Unerwartetes ist, das zu Auseinandersetzungen führt, in denen das Fachwissen nochmal einen anderen Zweck bekommt: Wie kann ich Fehler in der Technik, in der Argumentation der Akteure finden? Was muss ich darüber verstehen, um Fehler überhaupt erkennen zu können? Gerade auch das Scheitern an ersten Ideen beim Hands-On-Lernen hat bei vielen Lernenden sehr kreative Energien freigesetzt. Es ist ein induktives Lernen, das hier erfolgreich befördert wurde. Auch wenn Fingerabdruckbiometrie eine informatisch voraussetzungsvolle Technik ist, motiviert gerade ihre praktische kritische Infragestellung sowie ihre Einordnung in einen Diskurs anhand einer konkreten Anwendung, in dem sich bestimmte Argumente bei verschiedenen Akteuren immer wiederholen, sich das nötige Wissen besser zu erschließen.

Es zeigte sich insgesamt, dass es insbesondere beim diskursanalytischen Arbeiten größere Probleme gibt. Das argumentierende Bewerten etwa von Texten oder Filmen über konkrete Techniken aus verschiedenen Medien, das Einordnen von Äußerungen in bestimmte Interessen- und Machtgefüge und das eigene mündliche wie schriftliche Argumentieren hierzu sind Praktiken, die in der Informatik weniger geübt werden. Obwohl es für Informatikerinnen wichtig ist, IT-Systeme, ihren Sinn und ihre Folgen gesellschaftlich einzuordnen, wird es als ungewöhnlich empfunden, sich im Informatikunterricht/-seminar mit dem mündlichen und gar schriftlichen Argumentieren solcher Einordnungen zu beschäftigen – hier bestanden gerade bei den Studierenden größere Hemmungen und meines Erachtens auch Nachholbedarf.

Aber auch die prinzipiell analytisch-experimentelle Herangehensweise an die praktischen Probleme erfordern ein hohes Maß an Selbständigkeit, das moderiert, motiviert und ausgewertet werden muss. Hier ist das entwickelte Lehr- und Lernkonzept ins-

besondere im Rahmen der schulischen Lehre noch nicht genügend ausprobiert und ausgereift, kann aber zumindest prototypisch zur Verfügung gestellt werden.

Es bleibt zu hoffen, dass Lehransätze wie dieser, in denen sowohl humanistisches als auch technisches Denken zu verschränken gesucht werden, um das Menschen- und Gesellschaftsbild, das in einer Technik steckt, zu verstehen und klug verhandeln zu lernen, mehr Anklang in der Informatiklehre finden. Denn es geht um mehr als die Heranbildung von Informatikerinnen, die Rechner entwerfen, warten, programmieren, entwickeln und nach permanenten Automatisierungs- und Steuerungslösungen suchen können. Wichtig ist es ebenso, gut zu verstehen, wie Maschinen falsch benutzt werden und wann man sie besser gar nicht erst benutzt. Hierfür hat sich ein fehlergeleitetes und im guten Sinne die Kontroverse, das Argumentieren und Urteilen beförderndes Lernen, das zum kritischen Denken, Ausprobieren und Lernen aus dem experimentellen Scheitern anregt, als produktiv und horizonterweiternd erwiesen.

Abkürzungsverzeichnis

AFIS	Automatisiertes Fingerabdruckidentifizierungssystem
ANSI	American National Standards Institute
API	Application Programming Interface
BCC	Biometrics Consortium Conference
BDB	Biometric Data Block
BDR	Biometric Data Record
BioAPI	Biometric Application Programming Interface
BIP	Biometric Interworking Protocol
BIR	Biometric Information Record
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BKA	Bundeskriminalamt
BSP	Biometric Service Provider
BSI	Bundesamt für Sicherheit in der Informationstechnik
CASED	Center for Advanced Security Research Darmstadt
CAST	Competence Center for Applied Security Technology
CBEFF	Common Biometric Exchange Formats Framework
CCC	Chaos Computer Club
CCD	Charge-Coupled Device
CIA	Central Intelligence Agency
CJIS	Criminal Justice Information Services Division
CMOS	Complementary Metal-Oxide-Semiconductor
CORDIS	Community Research and Development Information Service
DARPA	Defense Advanced Research Projects Agency
DET	Detection Error Tradeoff
DHS	United States Department of Homeland Security
DIN	Deutsches Institut für Normung
EBF	European Biometrics Forum
EER	Equal Error Rate
EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Center
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FRR	False Rejection Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FpVTE	Fingerprint Vendor Technology Evaluation

Fraunhofer IGD	Fraunhofer-Institut für Graphische Datenverarbeitung
Fraunhofer SIT	Fraunhofer-Institut für Sichere Informationstechnologie
FTA	Failure to Acquire
FTAR	Failure-to-Acquire Rate
FTE	Failure to Enrol
FTER	Failure-to-Enrol Rate
FTC	Failure to Capture
FTD	Failure to Detect
FTP	Failure to Process
FVC	Fingerprint Verification Competition
GI	Gesellschaft für Informatik e. V.
GUI	Graphical User Interface
IAFIS	Integrated Automated Fingerprint Identification System
IAI	International Association for Identification
IBIA	International Biometrics and Identity Association
IBS	International Biometric Society
IKT	Informations- und Kommunikationstechnik
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers
IFIP	International Federation for Information Processing
INCITS	InterNational Committee for Information Technology Standards
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITL	Information Technology Laboratory
JRC	Joint Research Centre of the European Commission
JTC	Joint Technical Committee
MCS	Multiclassifier Systems
MINEX	Minutiae Interoperability Exchange
MTIT	Minutiae Template Interoperability Test
NAS	National Academy of Sciences
NIA	Normenausschuss Informationstechnik und Anwendungen
NIST	National Institute of Standards and Technology
NPL	National Physical Laboratory
NSA	National Security Agency
NSF	National Science Foundation
PAD	Presentation Attack Detection
PET	Privacy-Enhancing Technologies
ROC	Receiver Operation Characteristic
SB	Security Block

SBH	Standard Biometric Header
TFT	Thin-Film Transistors
SC37	Subcommittee 37 »Biometrics«
SDK	Software Development Kit
SlapSeg	Slap Fingerprint Segmentation Evaluation
SPI	Service Provider Interface
SVM	Support Vector Machines
SWGFAST	Scientific Working Group on Friction Ridge Analysis, Study and Technology
TeleTrusT	Bundesverband IT-Sicherheit e.V.
WSQ	Wavelet Scalar Quantization
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

Abbildungsverzeichnis

Tabellenverzeichnis

Hinweis zu Bildrechten

Einige Abbildungen und Tabellen sind von der Creative-Commons-Lizenz dieser Arbeit ausgenommen. Sie sind mit Erlaubnis der Rechteinhaber hier verwendet, bitte jeweils Copyright-Hinweise beachten:

© Elsevier B.V.:

- Abbildung 2.15

© IEEE:

- Abbildung 2.8,
- Abbildung 2.9

© ISO/IEC:

- Abbildung 2.16 und Abbildung 4.1 (unteres Schema):
  Wiedergegeben mit Erlaubnis des DIN Deutsches Institut für Normung e. V. Maßgebend für das Anwenden der ISO Standards ist deren Fassung mit dem neuesten Ausgabedatum, die bei der Beuth Verlag GmbH, Burggrafenstraße 6, 10787 Berlin, erhältlich sind.

© Springer-Verlag:

- Abbildung 2.4,
- Abbildung 2.6,
- Abbildung 2.10,
- Abbildung 2.12,
- Abbildung 3.7,
- Abbildung 4.2,
- Tabelle 3.1,
- Tabelle 3.2,
- Tabelle 4.1

Quellenverzeichnis

Literatur, technische Standards und Filme

Abernathy, William und Lee Tien (14. 09. 2003): *Biometrics: Who's Watching You?* Electronic Frontier Foundation. URL: https://www.eff.org/wp/biometrics-whos-watching-you (letzter Abruf am: 31. 07. 2017) (siehe S. 14).

Adams, Douglas (1987): *Dirk Gently's Holistic Detective Agency*. New York: Pocket Books (siehe S. 74).

Albrecht, Astrid, Michael Behrens, Tony Mansfield, Martin Walsh, Will McMeechan, Marek Rejman-Greene, Mario Savastano, Philip Statham, Christiane Schmidt und Ben Schouten (08. 12. 2003): *BioVision. Roadmap for Biometrics In Europe to 2010*. Report (E0303), Amsterdam. URL: https://www.researchgate.net/publication/277283593_BioVision_Roadmap_for_Biometrics_In_Europe_to_2010 (letzter Abruf am: 31. 07. 2017) (siehe S. 87).

Alexander, David (23. 11. 2015): *5.6 million fingerprints stolen in U.S. personnel data hack: government*. Reuters (online). URL: http://www.reuters.com/article/us-usa-cybersecurity-fingerprints-idUSKCN0RN1V820150923 (letzter Abruf am: 31. 07. 2017) (siehe S. 15).

Allinson, Nigel M. (2009): *Fingerprint Compression*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil Jain. Boston, MA: Springer US. Kap. Fingerprint Compression, S. 446–452. DOI: 10.1007/978-0-387-73003-5_53 (siehe S. 49).

Amery, Steven G., Eric Thomas Harley und Eric J. Malm (2004): *The Myth of "The Myth of Fingerprints"*. In: The UMAP Journal, 25 (3), hrsg. von Paul J. Campbell, S. 215–230. URL: http://eaton.math.rpi.edu/Faculty/Kramer/MCM/2004mcmsolutions.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 135).

ANSI/NIST-ITL 1-2011 (2011): *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*. NIST Special Publication 500-290. American National Standard for Information Systems (ANSI). URL: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136 (letzter Abruf am: 01. 08. 2017) (siehe S. 55, 70).

Aronson, Elliot und Shelley Patnoe (1997): *Cooperation in the classroom*. New York: Longman (siehe S. 216).

Artikel-29-Datenschutzgruppe (27. 04. 2012): *Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien*. 00720/12/DE. Version WP 193. URL: https://cnpd.public.lu/de/publications/groupe-art29/wp193_de.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 124).

Ashbaugh, David R. (1999): *Quantitative-qualitative friction ridge analysis: an introduction to basic and advanced ridgeology*. Boca Raton, New York: CRC press (siehe S. 31).

Ashbourn, Julian (2015): *Practical Biometrics*. 2nd (2004). London: Springer-Verlag (siehe S. 87).

Aus, Jonathan P. (2006): *Eurodac: A Solution Looking for a Problem?* In: European Integration online Papers (EIoP), 10. URL: http://eiop.or.at/eiop/texte/2006-006a.htm (letzter Abruf am: 31. 07. 2017) (siehe S. 124, 168).

Baier, Konrad (27. 02. 2013): *CeBIT 2013: Die biometrische Unterschrift bezahlt*. Pressemitteilung. Darmstadt, Rostock, Graz: Fraunhofer IGD. URL: https://www.pressebox.de/pressemitteilung/fraunhofer-institut-fuer-graphische-datenverarbeitung-igd-darmstadt/CeBIT-2013-Die-biometrische-Unterschrift-bezahlt/boxid/577177 (letzter Abruf am: 29. 07. 2017) (siehe S. 168).

Baldisserra, Denis, Annalisa Franco, Dario Maio und Davide Maltoni (2005): *Fake Fingerprint Detection by Odor Analysis*. In: *Proceedings International Conference on Biometrics (ICB) 2006, Hong Kong, China, January 5-7, 2006*. Hrsg. von D. Zhang und Anil K. Jain. Lecture Notes in Computer Science (LNCS) (3832), Berlin, Heidelberg: Springer-Verlag, S. 265–272 (siehe S. 53).

BAMF, Hrsg. (2012): *Dienstanweisung an das Asylverfahrenssekretariat (AVS) zur Ed-Behandlung mittels Fingerabdruckblatt (FABl)*. Bundesamt für Migration und Flüchtlinge (BAMF). URL: http://www.proasyl.de/fileadmin/fm-dam/NEWS/2013/Dienstanweisungen_Asyl_BAMF2013_Buchstabe_E.pdf (letzter Abruf am: 01. 08. 2017) (siehe S. 29).

Barthes, Roland (1964): *Mythen des Alltags*. Frankfurt am Main: Suhrkamp (siehe S. 134).

Bath, Corinna (2009): *De-Gendering informatischer Artefakte: Grundlagen einer kritisch-feministischen Technikgestaltung*. Dissertation. Universität Bremen. URL: http://elib.suub.uni-bremen.de/edocs/00102741-1.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 128).

Behrens, Michael und Richard Roth (2001): *Grundlagen und Perspektiven der biometrischen Identifikation*. In: *Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven*. Hrsg. von Michael Behrens und Richard Roth. DuD-Fachbeiträge. Wiesbaden: Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, S. 8–26 (siehe S. 34).

Bennett, Colin John und David Lyon, Hrsg. (2008): *Playing the Identity Card*. London und New York: Routledge (siehe S. 124).

Bertillon, Alphonse (1896): *Signaletic Instructions*. Übers. von R. W. McClaughry. Chicago, New York, London: The Werner Company. URL: https://archive.org/details/signaleticinstru00bert (letzter Abruf am: 23. 07. 2017) (siehe S. 97).

BEST Network (05. 07. 2010): *Inventory of European Training and Skills Provision*. Competitiveness and Innovation Framework Programme. Deliverable D5.1. Biometric European Stakeholder Network (BEST Network). URL: http://www.best-nw.eu/_fileupload/Deliverables/D5_1%20BEST%20Network.pdf (letzter Abruf am: 27. 10. 2014) (siehe S. 125).

Bigun, Josef (2009): *Fingerprint Features*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil Jain. Boston, MA: Springer US. Kap. Fingerprint Features, S. 465–473. DOI: 10.1007/978-0-387-73003-5_50 (siehe S. 49).

Biometric System Laboratory (25. 08. 2010): *Result of algorithm SourceAFIS 1.1 on FV-STD-1.0*. URL: https://biolab.csr.unibo.it/FvcOnGoing/UI/Form/AlgResult.aspx?algId=777 (letzter Abruf am: 31. 07. 2017) (siehe S. 93, 94).

Birolini, Alessandro (2004): *Reliability Engineering: Theory and Practice*. 4th (1994). Engineering online library. Berlin, Heidelberg: Springer (siehe S. 79).

BITKOM e. V., TeleTrusT e. V. und ZVEI e. V. (2008): *Landkarte Biometrie Deutschland*. Version 7.0 (siehe S. 152).

BITKOM e.V. (2008): *Biometrie. Referenzprojekte*. Hrsg. von Lutz Neugebauer und Leila Ambrosio. URL: http://www.bitkom.org/files/documents/Biometrie_Broschuere.pdf (letzter Abruf am: 27. 08. 2013) (siehe S. 152).

Bolle, Ruud M., Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha und Andrew W. Senior, Hrsg. (2004): *Guide to biometrics*. New York: Springer (siehe S. 27, 83, 84, 112–114, 133, 138, 139, 141, 144, 154, 155).

Borchers, Detlef (11. 08. 2003): *Heimatschutz durch Biometrie*. In: c't magazin für computertechnik, 17, S. 34. URL: https://www.cast-forum.de/presse/artikel/84 (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Borchers, Detlef und Jürgen Kuri (02. 03. 2004): *Biometrie für Flieger und Daheimgebliebene*. heise online. URL: http://heise.de/-94519 (letzter Abruf am: 29. 07. 2017) (siehe S. 159).

Brinda, Torsten, Michael Fothe, Steffen Friedrich, Bernhard Koerber, Hermann Puhlmann, Gerhard Röhner und Carsten Schulte (2008): *Grundsätze und Standards für die Informatik in der Schule. Bildungsstandards Informatik für die Sekundarstufe I*. In: LOG IN, 28 (150/151), hrsg. von Arbeitskreis »Bildungsstandards SII« des Fachausschusses »Informatische Bildung in Schulen« (FA IBS) und der Fachgruppe »Didaktik der Informatik« (FG DDI). URL: https://www.gi.de/fileadmin/redaktion/empfehlungen/Bildungsstandards_2008.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 182, 217).

Brömme, Arslan und Christoph Busch, Hrsg. (2003): *BIOSIG 2003. Proceedings of the 1st Conference on Biometrics and Electronic Signatures of the GI Working Group BIOSIG, Darmstadt, Germany, July 24*. P-31. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag. URL: http://subs.emis.de/LNI/Proceedings/Proceedings31.html (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Brömme, Arslan, Christoph Busch und Detlef Hühnlein, Hrsg. (2007): *BIOSIG 2007. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Darmstadt, Germany, July 12-13*. P-108. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag. URL: http://subs.emis.de/LNI/Proceedings/Proceedings108.html (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Brömme, Arslan, Christoph Busch und Detlef Hühnlein, Hrsg. (2008): *BIOSIG 2008. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Darmstadt, Germany, September 11-12*. P-137. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag. URL: http://subs.emis.de/LNI/Proceedings/Proceedings137.html (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Brömme, Arslan, Christoph Busch und Detlef Hühnlein, Hrsg. (2009): *BIOSIG 2009. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Darmstadt, Germany, September 17-18*. P-155. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag. URL: http://subs.emis.de/LNI/Proceedings/Proceedings155/P-155.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Brömme, Arslan und Christoph Busch, Hrsg. (2010): *BIOSIG 2010. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Darmstadt, Germany, September 9-10.* P-164. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag. URL: http://subs.emis.de/LNI/Proceedings/Proceedings164.html (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Brömme, Arslan und Christoph Busch, Hrsg. (2011): *BIOSIG 2011. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Darmstadt, Germany, September 8-9.* P-191. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag. URL: http://subs.emis.de/LNI/Proceedings/Proceedings191.html (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Brömme, Arslan und Christoph Busch, Hrsg. (2012): *BIOSIG 2012. Proceedings of the 11th International Conference of the Biometrics Special Interest Group, September 6-7 in Darmstadt, Germany.* P-196. Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag. URL: https://subs.emis.de/LNI/Proceedings/Proceedings196/P-196.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Brömme, Arslan und Christoph Busch, Hrsg. (2013): *BIOSIG 2013. Proceedings of the 12th International Conference of Biometrics Special Interest Group, Darmstadt, Germany, September 4-6.* P-212. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Köllen Verlag. URL: http://subs.emis.de/LNI/Proceedings/Proceedings212.html (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Brömme, Arslan und Christoph Busch, Hrsg. (2014): *BIOSIG 2014. Proceedings of the 13th International Conference of Biometrics Special Interest Group, Darmstadt, Germany, September 10-12.* P-230. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag. URL: http://subs.emis.de/LNI/Proceedings/Proceedings230/P-230.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Brömme, Arslan, Christoph Busch, Christian Rathgeb und Andreas Uhl, Hrsg. (2015): *BIOSIG 2015. Proceedings of the 14th International Conference of the Biometrics Special Interest Group, Darmstadt, Germany, September 9-11.* P-245. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag. URL: http://subs.emis.de/LNI/Proceedings/Proceedings245/P-245.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

Brömme, Arslan, Christoph Busch, Christian Rathgeb und Andreas Uhl, Hrsg. (2016): *BIOSIG 2016. Proceedings of the 15th International Conference of the Biometrics Special Interest Group, Darmstadt, Germany, September 21-23.* P-260. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag. URL: https://subs.emis.de/LNI/Proceedings/Proceedings260/P-260.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 158).

BSI (o. J.): *Fingerabdruckerkennung*. Bundesamt für Sicherheit in der Informationstechnik (BSI). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Fingerabdruckerkennung%5C_pdf.pdf (letzter Abruf am: 20. 06. 2016) (siehe S. 30).

BSI (23. 08. 2005): *Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen - BioP II.* Öffentlicher Abschlussbericht. Version 2.0. Bundesamt für Sicherheit in der Informationstechnik (BSI). URL: http://www.bsi.bund.de/literat/studien/biop/biopabschluss2.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 159).

BSI, BKA und Fraunhofer IGD (06. 08. 2008): *Evaluierung biometrischer Systeme Fingerabdrucktechnologien – BioFinger. Öffentlicher Abschlussbericht.* Bericht. Version 1.1. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundeskriminalamt (BKA) und Fraunhofer Institut für Graphische Datenverarbeitung (IGD). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioFinger/BioFinger_I_I_pdf.pdf?__blob=publicationFile&v=1 (letzter Abruf am: 31. 07. 2017) (siehe S. 159).

Bundesministerium des Innern, Hrsg. (01. 11. 2007): *Elektronischer Reisepass. Besonderheiten bei der Aufnahme von Passfoto und Fingerabdrücken für den ePass.* URL: http://www.bmi.bund.de/cae/servlet/contentblob/122838/publicationFile/13143/ePass_BesonderheitenbeiAufnahme.pdf (letzter Abruf am: 01. 08. 2017) (siehe S. 15).

Burger, Bettina, Dana Fuchs, Eli Sprecher und Peter Itin (2011): *The immigration delay disease: Adermatoglyphia-inherited absence of epidermal ridges.* In: Journal of the American Academy of Dermatology, 64 (5), S. 974–980. DOI: 10.1016/j.jaad.2009.11.013. URL: http://www.sciencedirect.com/science/article/pii/S0190962209014753 (letzter Abruf am: 01. 08. 2017) (siehe S. 141).

Burkert, Herbert (1997): *Privacy-enhancing Technologies: Typology, Critique, Vision.* In: *Technology and Privacy: The New Landscape.* Hrsg. von Philip E. Agre und Marc Rotenberg. Cambridge, MA, USA: MIT Press, S. 125–142. URL: http://dl.acm.org/citation.cfm?id=275283.275288 (letzter Abruf am: 01. 08. 2017) (siehe S. 170, 171).

Busch, Christoph, Hrsg. (o. J.): *Harmonized Biometric Vocabulary.* URL: http://www.christoph-busch.de/standards.html (letzter Abruf am: 20. 07. 2017) (siehe S. 32, 36, 38, 39, 104).

Busch, Christoph und Greg Canon (2009): *Biometric Data Interchange Format, Standardization.* In: *Encyclopedia of Biometrics.* Hrsg. von Stan Z. Li und Anil K. Jain. Berlin, Heidelberg: Springer Verlag. DOI: 10.1007/978-0-387-73003-5 (siehe S. 70, 72).

Cappelli, Raffaele, Matteo Ferrara, Annalisa Franco und Davide Maltoni (2007): *Fingerprint verification competition 2006.* In: Biometric Technology Today, 15, S. 7–9. DOI: 10.1016/S0969-4765(07)70140-6 (siehe S. 82).

Cappelli, Raffaele, Matteo Ferrara, Davide Maltoni und Dario Maio (2015): *MCC Software Development Kit (SDK) - Version 2.0 – Documentation.* Italy: Biometric System Laboratory, Department of Computer Science und Engineering, University of Bologna. URL: http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=82&pathSubj=111%7C%7C8%7C%7C82&Req=& (letzter Abruf am: 01. 08. 2017) (siehe S. 69).

Cappelli, Raffaele, Alessandra Lumini, Dario Maio und Davide Maltoni (1999): *Fingerprint classification by directional image partitioning.* In: IEEE Transactions on Pattern Analysis and Machine Intelligence, 21 (5), S. 402–421. DOI: 10.1109/34.765653 (siehe S. 60).

Cappelli, Raffaele und Davide Maltoni (2010): *FVC-onGoing: On-line Evaluation of Fingerprint Recognition Algorithms.* In: *Proceedings International Biometric Performance Conference (IBPC2010), March 2010.* (Gaithersburg, Maryland) (siehe S. 82).

CCC, Chaos Computer Club e.V. (2004): *Wie kopiere ich einen Fingerabdruck?* Film. Produktion: Frank Rosengart. URL: http://chaosradio.ccc.de/media/video/ccc-fingerabdruck.m4v (letzter Abruf am: 16. 07. 2017) (siehe S. 15).

CCC, Chaos Computer Club e.V., Hrsg. (2005): *Erfassungs Union, Schnüffelrepublik Deutschland, Überwachungspass*. Die Datenschleuder. Das wissenschaftliche Fachblatt für Datenreisende (87), URL: http://chaosradio.ccc.de/media/ds/ds087.pdf (letzter Abruf am: 01. 08. 2017) (siehe S. 14).

Chen, Yi und Jean-Christophe Fondeur (2009): *Biometric Algorithms*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil K. Jain. Berlin, Heidelberg: Springer Verlag, S. 64–68. DOI: 10.1007/978-0-387-73003-5 (siehe S. 66).

Cherkassky, Vladimir, Jerome H. Friedman und Harry Wechsler, Hrsg. (1994): *From Statistics to Neural Networks*. NATO ASI Series: Series F (136), Theory and Pattern Recognition Applications. Berlin, Heidelberg: Springer (siehe S. 67).

CJIS, Criminal Justice Information Services (o. J.): *Recording Legible Fingerprints*. URL: https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/recording-legible-fingerprints (letzter Abruf am: 18. 07. 2017) (siehe S. 29).

CJIS, Criminal Justice Information Services Division und FBI, Federal Bureau of Investigation, Hrsg. (24. 09. 2007): *Electronic Biometric Transmission Specification*. Version 8.0. URL: https://www.fbibiospecs.cjis.gov/Document/Get?fileName=EBTSv8.0_20070924.pdf (letzter Abruf am: 01. 08. 2017) (siehe S. 105).

CJIS, Criminal Justice Information Services und FBI, Federal Bureau of Investigation, Hrsg. (02. 07. 2013): *Electronic Biometric Transmission Specification*. Version 10.0. URL: https://www.fbibiospecs.cjis.gov/Document/Get?fileName=Master%20EBTS%20v10%20-%20FINAL%2020130702.pdf (letzter Abruf am: 01. 08. 2017) (siehe S. 105).

Cogent Systems GmbH (15. 01. 2003): *The Cogent Systems/Steria European Commission's EURODAC Automated Fingerprint Identification System was Declared Operational on January 15, 2003*. URL: http://files.shareholder.com/downloads/COGT/0x0x101260/5caed9a7-e068-4527-aafa-3917ac309d54/145777.pdf (letzter Abruf am: 01. 08. 2017) (siehe S. 13).

Cole, Simon A. (2001): *Suspect Identities: A history of fingerprinting and criminal identification*. Cambridge, Mass: Harvard University Press (siehe S. 30, 97, 125).

Cole, Simon A. (2005a): *Does "Yes" Really Mean Yes? The Attempt to Close Debate on the Admissibility of Fingerprint Testimony*. In: Jurimetrics, 45 (4), S. 449–464. URL: http://www.jstor.org/stable/29762908 (letzter Abruf am: 01. 08. 2017) (siehe S. 142).

Cole, Simon A. (2005b): *More than Zero: Accounting for Error in Latent Fingerprint Identification*. In: Journal of Criminal Law & Criminology, 95 (3), S. 985–1078. URL: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7201&context=jclc (letzter Abruf am: 01. 08. 2017) (siehe S. 142).

Cole, Simon A. (2006): *"Implicit Testing": Can Casework Validate Forensic Techniques?* In: Jurimetrics, 46 (2), S. 117–128. URL: http://www.jstor.org/stable/29762925 (letzter Abruf am: 01. 08. 2017) (siehe S. 30).

coloprint GmbH, Hrsg. (2014/2015): *Das Beste für den Tatort. Kriminaltechnik und Forensik*. Düsseldorf. URL: http://www.youblisher.com/p/840088-coloprint-GmbH-Kriminaltechnik-und-Forensik-Katalog-2014-2015/ (letzter Abruf am: 01. 08. 2017) (siehe S. 29).

Columbus, Simon (07. 12. 2009): *Fingerabdrücke für Einreise chirurgisch verändert*. Netzpolitik.org. URL: http://netzpolitik.org/2009/fingerabdruecke-fuer-einreise-chirurgisch-veraendert/ (letzter Abruf am: 01. 08. 2017) (siehe S. 15).

Commission of the European Communities (05. 05. 2004): *First annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*. Commission Staff Working Paper (SEC (2004) 557), URL: http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/sec/2004/0557/COM_SEC(2004)0557_EN.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 13).

CORDIS, Community Research and Development Information Service (13. 06. 2005): *BioVisioN – roadmap to successful deployments from the user and system integrator perspective*. Project reference: IST-2001-38236. URL: http://cordis.europa.eu/project/rcn/63054_en.html (letzter Abruf am: 31. 07. 2017) (siehe S. 160).

CORDIS, Community Research and Development Information Service (09. 04. 2008a): *3D FACE*. Project ID: 026845. URL: http://cordis.europa.eu/project/rcn/78379_en.html (letzter Abruf am: 29. 07. 2017) (siehe S. 159).

CORDIS, Community Research and Development Information Service (09. 04. 2008b): *Minutiae template interoperability testing (MTIT)*. Project reference: 027351. URL: http://cordis.europa.eu/project/rcn/78375_en.html (letzter Abruf am: 01. 08. 2017) (siehe S. 92).

CORDIS, Community Research and Development Information Service (25. 04. 2017): *Biometric European Stakeholders Network*. Project reference: 238955. URL: http://cordis.europa.eu/project/rcn/191867_en.html (letzter Abruf am: 28. 07. 2017) (siehe S. 161, 162).

Coy, Wolfgang (2005): *Informatik… im Großen und Ganzen*. In: LOG IN, 25 (136/137), S. 17–23 (siehe S. 21).

Coy, Wolfgang (2009): *Unsichtbar wird der Fehler, wenn sich alle daran gewöhnt haben*. In: *Die Unordnung der Dinge. Eine Wissens- und Mediengeschichte des Unfalls*. Hrsg. von Christian Kassung. Bielefeld: transcript Verlag, S. 325–353. URL: http://waste.informatik.hu-berlin.de/Lehre/ss12/PS_UnzSys/coy_unsichtbare-fehler.pdf (letzter Abruf am: 01. 08. 2017) (siehe S. 79, 80).

Cukic, Bojan und Nick Bartlow (20. 09. 2005): *Biometric System Threats and Countermeasures. A Risk Based Approach*. Folien. Biometric Consortium Conference. URL: http://web.archive.org/web/20160322230714/http://www.biometrics.org/bc2005/Presentations/Conference/2%20Tuesday%20September%2020/Tue_Ballroom%20B/Cukic_Threats%20and%20countermeasures.pdf (letzter Abruf am: 01. 08. 2017) (siehe S. 112).

Cummins, Harold und Rebecca Wright Kennedy (1940): *Purkinje's observations (1823) on finger prints and other skin features*. In: Journal of Criminal Law and Criminology (1931-1951), 31 (3), S. 343–356 (siehe S. 31).

Cutro, Brent T. (2011): *Recording Living and Postmortem Friction Ridge Skin Exemplars*. In: *The Fingerprint Sourcebook*. Hrsg. von Alan McRoberts und Debbie McRoberts. U.S. Department of Justice, Office of Justice Programs, S. 4-1–4-18. URL: http://www.nij.gov/publications/pages/publication-detail.aspx?ncjnumber=225320 (letzter Abruf am: 02. 08. 2017) (siehe S. 29).

DG Information Society and Media, European Commission, Hrsg. (2008): *Call for proposals ICT PSP 2*. Version 2. URL: http://ec.europa.eu/information_society/activities/ict_psp/documents/gfa_tnv1.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 162).

Doddington, George, Walter Liggett, Alvin Martin, Mark Przybocki und Douglas Reynolds (1998): *SHEEP, GOATS, LAMBS and WOLVES: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation*. In: *Proceedings of the 5th International Conference on Spoken Language Processing (ICSLP), 30th November - 4th December*. Sydney, Australia. URL: http://mirlab.org/conference_papers/International_Conference/ICSLP%201998/PDF/SCAN/SL980608.PDF (letzter Abruf am: 02. 08. 2017) (siehe S. 116).

Dorizzi, Bernadette, Raffaele Cappelli, Matteo Ferrara, Dario Maio, Davide Maltoni, Nesma Houmani, Sonia Garcia-Salicetti und Aurélien Mayoue (2009): *Fingerprint and On-Line Signature Verification Competitions at ICB 2009*. In: *Third International Conference on Biometrics, ICB 2009, June 2-5, 2009*. 5558: *Advances in Biometrics*. (Alghero, Italy). Hrsg. von Massimo Tistarelli und Mark S. Nixon. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, S. 725–732 (siehe S. 92, 126).

Du, Eliza Yingzi (2013): *An Introduction to Biometrics*. In: *Biometrics. From Fiction to Practice*. Hrsg. von Eliza Yingzi Du. Singapore: Pan Stanford Publishing, S. 1–9 (siehe S. 46, 56, 138, 139).

Duda, Richard O., Peter E. Hart und David G. Stork (2001): *Pattern Classification*. 2nd. New York: John Wiley & Sons, Inc. (siehe S. 42).

Dunstone, Ted und Neil Yager (2009): *Biometric System and Data Analysis*. Hrsg. von Ted Dunstone und Neil Yager. New York: Springer Science+Business Media (siehe S. 14, 15, 33, 34, 76, 84–86, 91, 96–98, 101, 115, 117, 121, 154).

Engemann, Christoph (2013): *Write me down, make me real – zur Gouvernemedialität digitaler Identität*. In: *Quoten, Kurven und Profile: Zur Vermessung der sozialen Welt*. Hrsg. von Jan-Hendrik Passoth und Josef Wehner. Wiesbaden: Springer VS, S. 205–227. DOI: 10.1007/978-3-531-93139-5_11 (siehe S. 26).

erdgeist (29. 03. 2008): *Chaos Computer Club konkretisiert Biometrie-Debatte an Schäubles Fingerabdruck*. Chaos Computer Club e.V. (CCC). URL: http://www.ccc.de/updates/2008/schaubles-finger (letzter Abruf am: 18. 06. 2016) (siehe S. 15).

Erdoğmuş, Nesli und Sébastien Marcel (2014): *Introduction*. In: *Handbook of Biometric Anti-Spoofing. Trusted Biometrics Under Spoofing Attacks*. Hrsg. von Sébastien Marcel, Mark S. Nixon und Stan Z. Li. Advances in computer vision and pattern recognition. London: Springer-Verlag, S. 1–11 (siehe S. 170).

European Commission, Hrsg. (2005): *Contact Group Eurodac (EUROpean DACtylographic comparison system)*. Register of Commission Expert Groups and Other Similar Entities. URL: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=609 (letzter Abruf am: 02. 08. 2017) (siehe S. 13).

EVISCAN GmbH (2017): *Berührungslose Tatortspurensicherung*. Werbebroschüre. URL: https://www.eviscan.com/files/157/eviscan-brochure-de-lowres.pdf (letzter Abruf am: 22. 07. 2017) (siehe S. 50).

Fawcett, Tom (2006): *An introduction to ROC analysis*. In: Pattern Recognition Letters, 27 (8), S. 861–874. DOI: 10.1016/j.patrec.2005.10.010 (siehe S. 98).

Fenker, Samuel P. und Kevin W. Bowyer (2012): *Analysis of Template Aging in Iris Biometrics*. In: *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, S. 45–51. URL: https://www3.nd.edu/~kwb/Fenker_Bowyer_CVPRW_2012.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 140).

Ferrara, Matteo (2010): *Biometric Fingerprint Recognition Systems*. Lambert Academic Publishing. URL: http://amsdottorato.unibo.it/1234/1/TesiFinale_-_Matteo_Ferrara.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 81).

Fiebig, Tobias, Jan Krissler und Ronny Hänsch (2014): *Security Impact of High Resolution Smartphone Cameras*. In: *8th USENIX Workshop on Offensive Technologies (WOOT 14)*. San Diego, CA: USENIX Association. URL: https://www.usenix.org/conference/woot14/workshop-program/presentation/fiebig (letzter Abruf am: 02. 08. 2017) (siehe S. 15).

Fischer-Hübner, Simone (2001): *IT-Security and Privacy. Design and Use of Privacy-Enhancing Security Mechanisms*. 1958. Lecture Notes in Computer Science (LNCS). Berlin, Heidelberg: Springer-Verlag (siehe S. 153).

FRONTEX, Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedsstaaten der Europäischen Union (2007): *BIOPASS. Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports*. Warschau. URL: http://frontex.europa.eu/assets/Publications/Research/Biopass_Study.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 160).

FRONTEX, Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedsstaaten der Europäischen Union (2010): *BIOPASS II. Automated biometric border crossing systems based on electronic passports and facial recognition: RAPID and SmartGate*. Techn. Ber. Warsaw. URL: http://frontex.europa.eu/assets/Publications/Research/Biopass_Study_II.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 160).

Galton, Francis (1892): *Finger Prints*. London und New York: Macmillian und Co. (siehe S. 31, 136).

Garfunkel, Solomon A. (2004): *Publisher's Editorial. The Good Fight*. In: The UMAP Journal, 25 (3), hrsg. von Paul J. Campbell, S. 185–188. URL: http://eaton.math.rpi.edu/Faculty/Kramer/MCM/2004mcmsolutions.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 134).

Gelb, Alan und Julia Clark (28. 01. 2013): *Identification for Development: the Biometrics Revolution*. Working Paper 315. URL: https://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 35).

Germain, Jack M. (04. 10. 2004): *IBM Introducing Fingerprint Reader into Laptop*. TechNewsWorld (online). URL: http://www.technewsworld.com/story/37017.html (letzter Abruf am: 02. 08. 2017) (siehe S. 35).

Gigerenzer, Gerd und Ulrich Hoffrage (1995): *How to improve Bayesian reasoning without instruction: frequency formats*. In: Psychological Review, 102 (4), S. 684–704 (siehe S. 102).

Goldstein, James, Rina Angeletti, Manfred Holzbach, Daniel Konrad und Max Snijder (2008): *Large-scale Biometrics Deployment in Europe. Identifying Challenges and Threats*. Report (EUR 23564 EN), European Commission. Joint Research Centre. Institute for Prospective Technological Studies. URL: http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=1899 (letzter Abruf am: 02. 08. 2017) (siehe S. 124, 140).

Golembiewski, Claudia und Thomas Probst (2003): *Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen*. Unabhängiges Landeszentrum für Datenschutz (ULD). URL: https://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 14).

Gonzalez, Rafael C. und Richard E. Woods (2007): *Digital Image Processing*. 3rd. New Jersey: Prentice-Hall (siehe S. 41, 44).

González-Agulla, Elisardo, Enrique Otero-Muras, Carmen García-Mateo und José Luis Alba-Castro (2009): *A multiplatform Java wrapper for the BioAPI framework*. In: Computer Standards & Interfaces, 31 (1), S. 186–191. DOI: 10.1016/j.csi.2007.11.004 (siehe S. 70).

Gramm, Andreas, Malte Hornung und Helmut Witten (2011): *E-Mail (nur?) für Dich. Eine Unterrichtsreihe des Projekts Informatik im Kontext*. In: LOG IN, 31 (169/170). URL: http://medienwissenschaft.uni-bayreuth.de/informatik-im-kontext/assets/Entwuerfe-Material/E-Mail-nur-fuer-dich/LOGIN169-1702011BEILAGEIniK.PDF? (letzter Abruf am: 02. 08. 2017) (siehe S. 173).

Hahn, Benjamin (18. 07. 2015): *Fingerabdruckscan beim Erkennungsdienst der Polizei. Digitale Verbrecherjagd*. Ruhrnachrichten.de. URL: http://www.ruhrnachrichten.de/staedte/bochum/Digitale-Verbrecherjagd-Fingerabdruckscan-beim-Erkennungsdienst-der-Polizei;art932,2766427 (letzter Abruf am: 02. 08. 2017) (siehe S. 29).

Haller, Dieter (19. 04. 2004): *Vom Digitalen Ausweis zur Spracherkennung an der Tür*. In: eGoverment Computing. Die Zeitung für IT-gestützte Verwaltung von Kommune und Staat, 4 (5), S. 20 (siehe S. 13).

Hara, Masanori (2009): *Fingerprint Image Enhancement*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil Jain. Boston, MA: Springer US. Kap. Fingerprint Image Enhancement, S. 474–482. DOI: 10.1007/978-0-387-73003-5_49 (siehe S. 49).

Hartmann, Werner, Michael Näf und Raimond Reichert (2007): *Informatikunterricht planen und durchführen*. eXamen.press. Berlin, Heidelberg: Springer (siehe S. 173, 217, 223).

Haustein, Heinz Dieter (2001): *Weltchronik des Messens*. Berlin, New York: De Gruyter (siehe S. 167).

Hayes, Ben (2009): *NeoConOpticon. The EU Security-Industrial Complex*. Studie. Transnational Institute (TNI) und Statewatch. URL: http://www.statewatch.org/analyses/neoconopticon-report.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 168).

Heindl, Robert (1927): *System und Praxis der Daktyloskopie und der sonstigen technischen Methoden der Kriminalpolizei*. 3. überarbeitete und erweiterte Auflage. Berlin, Leipzig: Walter de Gruyter & Co. (siehe S. 31).

Hellige, Hans Dieter (1996): *Technikleitbilder als Analyse-, Bewertungs- und Steuerungsinstrumente: Eine Bestandsaufnahme aus informatik- und computerhistorischer Sicht*. In: *Technikleitbilder auf dem Prüfstand. Das Leitbild-Assessment aus Sicht der Informatik- und Computergeschichte*. Hrsg. von Hans Dieter Hellige. Berlin: edition sigma, S. 15–37. URL: http://www.uni-bremen.de/fileadmin/user_upload/single_sites/artec/artec_Dokumente/Hellige_1996_Technikleitbilder-Bestandsaufnahme.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 19).

Henry, Edward Richard (1900): *Classification and Uses of Fingerprints*. London: George Routledge und Sons, Ltd. URL: https://archive.org/details/classificationa01henrgoog (letzter Abruf am: 02. 08. 2017) (siehe S. 31).

Hicklin, Austin, Brad Ulery und Craig Watson (2005): *The Myth of Goats: How many people have fingerprints that are hard to match?* NIST Interagency Report (NISTIR) (7271), National Institute of Standards und Technology (NIST). URL: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=150390 (letzter Abruf am: 02. 08. 2017) (siehe S. 141).

Hong, Lin, Yifei Wan und Anil K. Jain (1998): *Fingerprint image enhancement: algorithm and performance evaluation*. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, 20 (8), S. 777–789. DOI: 10.1109/34.709565 (siehe S. 60).

Hornung, Gerrit (2005): *Die digitale Identität*. Der elektronische Rechtsverkehr (10), Baden-Baden: Nomos Verlagsgesellschaft (siehe S. 124).

Hornung, Gerrit (2007): *The European Regulation on Biometric Passports. Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*. In: SCRIPTed, 4 (3). DOI: 10.2966/scrip.040307.246 (siehe S. 154).

Hummel, Diana (2000): *Die Population als Gegenstand der Wissenschaft*. In: *Der Bevölkerungsdiskurs*. Forschung Politikwissenschaft (108), VS Verlag für Sozialwissenschaften, S. 187–212. DOI: 10.1007/978-3-663-09594-1_7 (siehe S. 26).

Hutchins, Laura A. (2011): *Systems of Friction Ridge Classification*. In: *The Fingerprint Sourcebook*. Hrsg. von Alan McRoberts und Debbie McRoberts. U.S. Department of Justice, Office of Justice Programs, S. 5-1–5-25. URL: http://www.nij.gov/publications/pages/publication-detail.aspx?ncjnumber=225320 (letzter Abruf am: 02. 08. 2017) (siehe S. 31).

ICAO, International Civil Aviation Organization (2008): *Doc 9303, Machine Readable Travel Documents, Part 3: Machine Readable Official Travel Documents, Volume 2: Specifications for Electronically Enabled MRtds with Biometric Identification Capability*. 3rd Edition. International Civil Aviation Organization (siehe S. 82).

International Biometric Society (o. J.): *Definition of Biometrics*. URL: http://www.biometricsociety.org/about/definition-of-biometrics/ (letzter Abruf am: 02. 08. 2017) (siehe S. 27).

ISO/IEC 19784-1:2006/Amd 1:2007 (2007): *Information technology – Biometric application programming interface – Part 1: BioAPI specification, Amendment 1: BioGUI specification*. Standard. Geneva: International Organization for Standardization (siehe S. 49).

ISO/IEC 19785-1:2015 (01. 08. 2015): *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*. Standard. Geneva: International Organization for Standardization (siehe S. 108).

ISO/IEC 19785-2:2006 (15. 04. 2006): *Information technology – Common Biometric Exchange Formats Framework – Part 2: Procedures for the operation of the Biometric Registration Authority*. Standard. Geneva: International Organization for Standardization (siehe S. 108).

ISO/IEC 19785-3:2015 (01. 09. 2015): *Information technology – Common Biometric Exchange Formats Framework – Part 3: Patron format specifications*. Standard. Geneva: International Organization for Standardization (siehe S. 108).

ISO/IEC 19785-4:2010 (15. 08. 2010): *Information technology – Common Biometric Exchange Formats Framework – Part 4: Security block format specifications*. Standard. Geneva: International Organization for Standardization (siehe S. 108).

ISO/IEC 19794-1:2011/Amd 1:2013 (01. 02. 2013): *Information technology – Biometric data interchange formats – Part 1: Framework – Amendment 1: Conformance testing methodology*. Standard. Geneva: International Organization for Standardization (siehe S. 108).

ISO/IEC 19794-2:2011 (12/2011): *Information technology – Biometric data interchange formats – Part 2: Finger minutiae data*. Standard. Geneva: International Organization for Standardization (siehe S. 63, 92).

ISO/IEC 19794-2:2011/Amd 1:2013 (01. 12. 2013): *Information technology – Biometric data interchange formats – Part 2: Finger minutiae data – Amendment 1: Conformance testing methodology and clarification of defects*. Standard. Geneva: International Organization for Standardization (siehe S. 108).

ISO/IEC 19794-4:2011/Amd 1:2013 (15. 06. 2013): *Information technology – Biometric data interchange formats – Part 4: Finger image data – Amendment 1: Conformance testing methodology and clarification of defects*. Standard. Geneva: International Organization for Standardization (siehe S. 108).

ISO/IEC 19794-8:2011/Amd 1:2014 (01. 04. 2014): *Information technology – Biometric data interchange formats – Part 8: Finger pattern skeletal data – Amendment 1: Conformance testing methodology*. Standard. Geneva: International Organization for Standardization (siehe S. 108).

ISO/IEC 19795-1:2006 (01. 04. 2006): *Information Technology – Biometric performance testing and reporting – Part I: Principles and framework*. Standard. Geneva: International Organization for Standardization (siehe S. 75, 92, 95, 99, 108–110, 117).

ISO/IEC 2382-37:2017 (02/2017): *Information technology – Vocabulary – Part 37: Biometrics*. Standard. Geneva: International Organization for Standardization. URL: http://standards.iso.org/ittf/PubliclyAvailableStandards/c066693_ISO_IEC_2382-37_2017.zip (letzter Abruf am: 20. 07. 2017) (siehe S. 25, 32, 33, 36, 39, 75, 99, 104, 106, 121, 138, 139, 151).

ISO/IEC 24708:2008 (15. 12. 2008): *Information technology – Biometrics – BioAPI Interworking Protocol*. Standard. Geneva: International Organization for Standardization (siehe S. 70).

ISO/IEC 24745:2011 (2011): *Information technology – Security techniques – Biometric information protection*. Standard. Geneva: International Organization for Standardization (siehe S. 55).

ISO/IEC 24779-1:2016 (04/2016): *Information technology – Cross-jurisdictional and societal aspects of implementation of biometric technologies – Pictograms, icons and symbols for use with biometric systems – Part 1: General principles*. Standard. Geneva: International Organization for Standardization (siehe S. 49, 111).

ISO/IEC 24779-4:2017 (01/2017): *Information technology – Cross-jurisdictional and societal aspects of implementation of biometric technologies – Pictograms, icons and symbols for use with biometric systems – Part 4: Fingerprint applications*. Standard. Geneva: International Organization for Standardization (siehe S. 49, 111).

ISO/IEC AWI TR 20322 (2015): *Information technology – Cross jurisdictional and societal aspects of implementation of biometric technologies – Biometrics and Elderly*. Standard under development. Geneva: International Organization for Standardization (siehe S. 111).

ISO/IEC JTC 1/SC 37 N 3972 (16. 08. 2010): *Text of Standing Document 11 (SD 11). Part 1 Overview Standards Harmonization Document*. Standing Document N 3972. Geneva: International Organization for Standardization (siehe S. 144, 145).

ISO/IEC JTC 1/SC 37 N 5831 (28. 01. 2014): *Approved Resolutions from the January 2014 SC 37 Plenary Meeting in Darmstadt, Germany*. Geneva: International Organization for Standardization (siehe S. 144).

ISO/IEC TR 24741:2007 (2007): *Information technology - Biometrics tutorial*. Geneva: International Organization for Standardization (siehe S. 33, 34, 40, 43, 46–48, 71, 101, 110, 118, 144, 145, 147–149).

ISO/IEC TR 29156:2015 (11/2015): *Information technology – Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics*. Geneva: International Organization for Standardization. URL: https://www.iso.org/standard/45235.html?browse=tc (letzter Abruf am: 22. 07. 2017) (siehe S. 49).

ISO/IEC TR 30110:2015 (04. 11. 2015): *Information technology – Cross jurisdictional and societal aspects of implementation of biometric technologies – Biometrics and children*. Geneva: International Organization for Standardization (siehe S. 111).

ISO/IEC TR 24714-1:2008 (15. 12. 2008): *Information technology - Biometrics - Jurisdictional and societal considerations for commercial applications - Part 1: General guidance*. Geneva: International Organization for Standardization (siehe S. 111).

Jäger, Margarete (2008): *Diskursanalyse: Ein Verfahren zur kritischen Rekonstruktion von Machtbeziehungen*. In: *Handbuch Frauen- und Geschlechterforschung: Theorie, Methoden, Empirie*. Hrsg. von Ruth Becker und Beate Kortendiek. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 378–383. DOI: 10.1007/978-3-531-91972-0_45 (siehe S. 176).

Jäger, Siegfried (2012): *Kritische Diskursanalyse*. 6. Auflage (1993). Edition DISS. Münster: Unrast Verlag (siehe S. 20, 21).

Jähne, Bernd (2012): *Digitale Bildverarbeitung*. 7., neu bearbeitete Auflage. Berlin, Heidelberg: Springer Vieweg (siehe S. 41, 45, 60).

Jain, Anil K., Sarat C. Dass und Karthik Nandakumar (2004): *Can soft biometric traits assist user recognition?* In: *Biometric Technology for Human Identification*. Hrsg. von Anil K. Jain und Nalini K. Ratha. 5404. Proceedings of SPIE. Orlando, FL, S. 561–572. URL: http://cse.msu.edu/rgroups/biometrics/Publications/SoftBiometrics/JainDassNandakumar_SoftBiometrics_SPIE04.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 123).

Jain, Anil K., Jianjiang Feng und Karthik Nandakumar (2010): *Fingerprint Matching*. In: Computer, 43 (2), S. 36–44. DOI: 10.1109/MC.2010.38 (siehe S. 170).

Jain, Anil K., Patrick Flynn und Arun A. Ross, Hrsg. (2008a): *Handbook of Biometrics*. New York: Springer Science+Business Media (siehe S. 40, 104, 146, 147).

Jain, Anil K., Patrick Flynn und Arun A. Ross (2008b): *Introduction to Biometrics*. In: *Handbook of Biometrics*. Hrsg. von Anil K. Jain und Arun A. Ross. New York: Springer Science+Business Media, S. 1–22 (siehe S. 117, 120).

Jain, Anil K. und Karthik Nandakumar (2009): *Biometric System Design, Overview*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil K. Jain. Berlin, Heidelberg: Springer Verlag, S. 135–140. DOI: 10.1007/978-0-387-73003-5_183 (siehe S. 83, 84, 89).

Jain, Anil K., Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun A. Ross und James L. Wayman (2004): *Biometrics: A Grand Challenge*. In: *Proceedings of the 17th International Conference on Pattern Recognition, Cambridge, August 2004*. 2, S. 935–942. DOI: 10.1109/ICPR.2004.1334413 (siehe S. 96).

Jain, Anil K. und Arun A. Ross (2004): *Multibiometric Systems*. In: Commun. ACM, 47 (1), S. 34–40. DOI: 10.1145/962081.962102 (siehe S. 140).

Jain, Anil K., Arun A. Ross und Sharath Pankanti (2006): *Biometrics: a tool for information security*. In: Information Forensics and Security, IEEE Transactions on, 1 (2), S. 125–143 (siehe S. 86, 112).

Käser, Udo (2011): *Fehler begehen – Mathematik verstehen. Über die Bedeutung von Fehlern für das Verstehen*. In: *Mathematik Verstehen. Philosophische und Didaktische Perspektiven*. Hrsg. von Markus Helmerich, Katja Lengnink, Gregor Nickel und Martin Rathgeb. Wiesbaden: Vieweg+Teubner, S. 167–178. DOI: 10.1007/978-3-8348-9836-4_13 (siehe S. 178).

Kaseva, Antti und Antti Stén (24. 03. 2003a): *Fooling Fingerprint Scanners. Biometric vulnerabilities of the Precise Biometrics 100 SC scanner*. Helsinki University of Technology. URL: www.cil.cnrs.fr/CIL/IMG/pdf/GiveMeAFinger.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 15, 190).

Kaseva, Antti und Antti Stén (18. 03. 2003b): *Hacking Biometrics. Fooling A Fingerprint Scanner 2/3: Creating an artificial finger using the actual finger*. URL: https://web.archive.org/web/20140301024350/http://stdot.com:80/pub/ffs/hack2.html (letzter Abruf am: 02. 08. 2017) (siehe S. 196).

Kaseva, Antti und Antti Stén (18. 03. 2003c): *Hacking Biometrics. Fooling A Fingerprint Scanner 3/3: Creating an artificial finger using a latent fingerprint*. URL: https://web.archive.org/web/20140209161354/http://www.stdot.com:80/pub/ffs/hack3.html (letzter Abruf am: 02. 08. 2017) (siehe S. 195, 198).

Kevenaar, Tom, Ulrike Korte, Johannes Merkle, Matthias Niesing, Heinrich Ihmor, Christoph Busch und Xuebing Zhou (2010): *A reference framework for the privacy assessment of keyless biometric template protection systems*. In: *BIOSIG 2010. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Darmstadt, Germany, September 9-10*. Hrsg. von Arslan Brömme und Christoph Busch. P-164. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag, S. 45–56. URL: https://subs.emis.de/LNI/Proceedings/Proceedings164/article5603.html (letzter Abruf am: 02. 08. 2017) (siehe S. 113).

Kindt, Els J. (2013): *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*. Law, Governance and Technology Series. Springer Netherlands (siehe S. 118, 124, 152).

Knaut, Andrea (2013): *Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen. Kommentiertes Protokoll der Tagung*. In: *Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen, Workshop HU, 30.10.-1.12.2012*. (Berlin, Humboldt-Universität). Hrsg. von Andrea Knaut. Arbeitsgruppe »Informatik in Bildung und Gesellschaft«, S. 61–99. URL: http://edoc.hu-berlin.de/conferences/bioident/all/bioident2013.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 101).

Knuth, Donald E. (1989): *The Errors of TEX*. In: Software: Practice and Experience, 19 (7), S. 607–685. DOI: 10.1002/spe.4380190702 (siehe S. 178).

Knuth, Donald E. (1992): *Learning from our Errors*. In: *Software Development and Reality Construction*. Hrsg. von Christiane Floyd, Heinz Züllighoven, Reinhard Budde und Reinhard Keil-Slawik. Berlin, Heidelberg: Springer, S. 28–30. DOI: 10.1007/978-3-642-76817-0_3 (siehe S. 178).

Kolb, David A. (1985): *Learning Style Inventory*. Boston: McBer und Company (siehe S. 177).

Koubek, Jochen (2005): *Informatische Allgemeinbildung*. In: *Unterrichtskonzepte für informatische Bildung, INFOS 2005, 11. GI-Fachtagung Informatik und Schule, 28.-30. September 2005 an der TU Dresden*. Hrsg. von Steffen Friedrich. P-60. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag, S. 57–66. URL: http://subs.emis.de/LNI/Proceedings/Proceedings60/article4230.html (letzter Abruf am: 02. 08. 2017) (siehe S. 174, 175).

Koubek, Jochen, Ira Diethelm und Helmut Witten (2011): *IniK — Informatik im Kontext, Entwicklungen, Merkmale und Perspektiven*. In: LOG IN, 169/170 (siehe S. 21, 22).

Koubek, Jochen und Jens-Martin Loebel (2007): *Informatik & Informationsgesellschaft II: Technik, Geschichte und Kontext. 02–Diskursanalyse*. Folien. [Passwort der Folien ist "iundg"]. URL: http://waste.informatik.hu-berlin.de/Lehre/ss07/IuIG/Vorlesungen/02_Diskursanalyse.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 175).

Koubek, Jochen, Carsten Schulte, Peter Schulze und Helmut Witten (2009): *Informatik im Kontext (IniK). Ein integratives Unterrichtskonzept für den Informatikunterricht*. In: *Proceedings of the 13. GI-Fachtagung Informatik und Schule, 21. 9. – 24.9.2009, Berlin. Zukunft braucht Herkunft*. Hrsg. von Bernhard Koerber. P-156. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag, S. 268–279. URL: http://medienwissenschaft.uni-bayreuth.de/inik/material/InformatikImKontextINFOS2009.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 19).

Krasmann, Susanne und Sylvia Kühne (2014): *'My fingerprint on Osama's cup'. On objectivity and the role of the fictive regarding the acceptance of a biometric technology*. In: Surveillance & Society, 12 (1), URL: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/fingerprint/osamas-cup (letzter Abruf am: 02. 08. 2017) (siehe S. 133, 134).

Krempl, Stefan (28. 12. 2014): *31C3: CCC-Tüftler hackt Merkels Iris und von der Leyens Fingerabdruck*. heise online. URL: https://heise.de/-2506929 (letzter Abruf am: 30. 07. 2017) (siehe S. 220).

Kuster, Brigitta und Vassilis S. Tsianos (2013): *»How to liquefy a moving body: Eurodac und die Digitalisierung der Europäischen Grenze«*. In: *Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen, Workshop HU, 30.10.-1.12.2012*. (Berlin, Humboldt-Universität). Hrsg. von Andrea Knaut. Arbeitsgruppe »Informatik in Bildung und Gesellschaft«, S. 19–36. URL: http://edoc.hu-berlin.de/conferences/bioident/all/bioident2013.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 121, 124).

Kwon, Young-Bin (22. 09. 2009): *Biometrics in Asia. Presentation on the Biometric Consortium Conference, 2009*. Folien. URL: https://web.archive.org/web/20101011051437/http://biometrics.org/bc2009/presentations/tuesday/Kwon%20MR%2014%20Tue%20345%20PM%20-%20400%20PM.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 169).

Larmouth, John (2009): *Biometric Technical Interface, Standardization*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil K. Jain. Berlin, Heidelberg: Springer Verlag, S. 145–152. DOI: 10.1007/978-0-387-73003-5_231 (siehe S. 108).

Latour, Bruno (2006): *Technik ist stabilisierte Gesellschaft*. In: *ANThology. Ein einführendes Handbuch zur Akteur-Netzwerk-Theorie*. Hrsg. von Andréa Belliger und David J. Krieger. Bielefeld: transcript Verlag, S. 369–397 (siehe S. 20).

Lazarick, Rick (18. 09. 2012): *SC37 Project 30107 Presentation Attack Detection*. Slides. URL: http://biometrics.org/bc2012/presentations/Standards/Standards_Tue_1105-1130_Lazarick.pdf (letzter Abruf am: 15. 10. 2013) (siehe S. 118).

Li, Stan Z. und Anil K. Jain, Hrsg. (2009): *Encyclopedia of Biometrics*. Berlin, Heidelberg: Springer Verlag. DOI: 10.1007/978-0-387-73003-5 (siehe S. 49).

Loctier, Denis (17. 03. 2014): *Behind the mask of biometric security*. Artikel plus Filmbeitrag. euronews (online). URL: http://www.euronews.com/2014/03/17/behind-the-mask-of-biometric-security (letzter Abruf am: 17. 07. 2017) (siehe S. 15).

Loyola-González, Octavio, Miguel Angel Medina-Pérez, Andres Eduardo Gutierrez-Rodríguez und Milton García-Borroto (20. 11. 2015): *A Framework in C# for Fingerprint Verification*. URL: http://www.codeproject.com/Articles/97590/A-Framework-in-C-for-Fingerprint-Verification (letzter Abruf am: 02. 08. 2017) (siehe S. 126).

Lu, Yipeng, Hao-Yen Tang, Stephanie Fung, Qi Wang, Julius M. Tsai, Michael J. Daneman, Bernard E. Boser und David A. Horsley (2015): *Ultrasonic fingerprint sensor using a piezoelectric micromachined ultrasonic transducer array integrated with complementary metal oxide semiconductor electronics*. In: Applied Physics Letters, 106 (26), 263503. DOI: 10.1063/1.4922915. URL: https://www.researchgate.net/publication/281321246_Ultrasonic_fingerprint_sensor_using_a_piezoelectric_micromachined_ultrasonic_transducer_array_integrated_with_complementary_metal_oxide_semiconductor_electronics (letzter Abruf am: 02. 08. 2017) (siehe S. 53).

Lumini, Alessandra, Loris Nanni und Davide Maltoni (2010): *Learning in Fingerprints*. In: *Biometrics. Theory, Methods, and Applications*. Hrsg. von Nikolaos v. Boulgouris, Konstantinos N. Plataniotis und Evangelia Micheli-Tzanakou. IEEE Press Series on Computational Intelligence. Hoboken, New Jersey: John Wiley & Sons, S. 339–364 (siehe S. 67, 68, 104).

Lynch, Jennifer (2012): *From Fingerprints to DNA. Biometric Data Collection in U.S. Immigrant Communities and Beyond*. Report. Electronic Frontier Foundation, Immigration Policy Center. URL: https://www.eff.org/document/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond (letzter Abruf am: 02. 08. 2017) (siehe S. 14).

Lyon, David (1994): *The Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press (siehe S. 171).

Lyon, David (2002): *Surveillance Studies: understanding visibility, mobility and the phenetic fix*. In: Surveillance & Society, 1 (1), S. 1–7 (siehe S. 17).

Lyon, David (2013): *Identifying Citizens*. John Wiley & Sons (siehe S. 124).

Mackensen, Rainer (2002): *Demographie als Wissenschaft*. In: Sitzungsberichte der Leibniz-Sozietät, 51 (8), S. 87–130. URL: http://leibnizsozietaet.de/wp-content/uploads/2012/11/07_mackensen.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 26).

Mackensen, Rainer, Hrsg. (2006): *Bevölkerungsforschung und Politik in Deutschland im 20. Jahrhundert*. Wiesbaden: VS Verlag für Sozialwissenschaften (siehe S. 26).

Mackensen, Rainer und Jürgen Reulecke, Hrsg. (2005): *Das Konstrukt „Bevölkerung" vor, im und nach dem „Dritten Reich"*. Wiesbaden: VS Verlag für Sozialwissenschaften (siehe S. 26).

Maghiros, Ioannis, Yves Punie, Sabine Delaitre, Elsa Lignos, Carlos Rodríguez, Martin Ulbrich, Marcelino Cabrera, Bernard Clements, Laurent Beslay und Rene van Bavel (2005): *Biometrics at the Frontiers. Assessing the Impact on Society*. For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE). Technical Report (EUR 21585 EN), Spain: European Commission Joint Research Centre, Institute for Prospective Technological Studies. URL: http://ftp.jrc.es/EURdoc/eur21585en.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 124, 160).

Maltoni, Davide, Dario Maio, Anil K. Jain und Salil Prabhakar (2009): *Handbook of fingerprint recognition*. 2nd. London: Springer-Verlag (siehe S. 14, 25, 28, 30, 33, 37, 40, 41, 49, 51, 55–67, 75, 76, 80, 84–86, 88, 93, 94, 96, 97, 99, 100, 104, 106, 107, 112, 120, 122, 123, 136, 137, 140, 142, 146, 148, 149, 167–169, 227).

Mansfield, A. J. und James L. Wayman (2002): *Best Practices in Testing and Reporting Performance of Biometric Devices*. NPL Report CMSC 14/02. Version 2.01. Centre for Mathematics und Scientific Computing, National Physical Laboratory. URL: http://www.idsysgroup.com/ftp/BestPractice.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 140, 145).

Marcel, Sébastien, Mark S. Nixon und Stan Z. Li, Hrsg. (2014): *Handbook of Biometric Anti-Spoofing. Trusted Biometrics Under Spoofing Attacks*. Advances in computer vision and pattern recognition. London: Springer-Verlag (siehe S. 15).

Massen, Robert (1996): *Sehen, Erkennen, Entscheiden*. In: Jähne, Bernd, Robert Massen, Bertram Nickolay und Harald Scharfenberg. *Technische Bildverarbeitung – Maschinelles Sehen*. Berlin, Heidelberg: Springer-Verlag, S. 1–34 (siehe S. 41).

Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada und Satoshi Hoshino (2002): *Impact of Artificial "Gummy" Fingers on Fingerprint Systems*. In: *SPIE Proceedings*. Hrsg. von Rudolf L. van Renesse. 4677. Optical Security and Counterfeit Deterrence Techniques IV, S. 275–289. DOI: 10.1117/12.462719. URL: http://cryptome.org/gummy.htm (letzter Abruf am: 02. 08. 2017) (siehe S. 15).

McIver, Rene (2009): *Biometric Vocabulary, Standardization*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil K. Jain. Berlin, Heidelberg: Springer Verlag, S. 157–160. DOI: 10.1007/978-0-387-73003-5_227 (siehe S. 119).

Medina-Pérez, Miguel Angel, Octavio Loyola-González, Andres Eduardo Gutierrez-Rodríguez, Milton García-Borroto und Leopoldo Altamirano-Robles (2014): *Introducing an Experimental Framework in C# for Fingerprint Recognition*. In: *Pattern Recognition*. Hrsg. von José Francisco Martínez-Trinidad, Jesús Ariel Carrasco-Ochoa, José Arturo Olvera-Lopez, Joaquín Salas-Rodríguez und Ching Y. Suen. 8495. Lecture Notes in Computer Science (LNCS). Cham: Springer International Publishing, S. 132–141. DOI: 10.1007/978-3-319-07491-7_14 (siehe S. 127).

Meffert, Beate und Olaf Hochmuth (2004): *Werkzeuge der Signalverarbeitung*. München: Addison-Wesley Verlag (siehe S. 41, 45).

Meßner, Daniel (2015): *Die Erfindung der Biometrie – Identifizierungstechniken und ihre Anwendungen, 1870–1914*. Dissertation. Universität Wien. URL: http://othes.univie.ac.at/39278/1/2015-07-21_0303769.pdf (letzter Abruf am: 26. 07. 2017) (siehe S. 124).

Meyer, Hilbert (2014): *Leitfaden Unterrichtsvorbereitung*. 8. Auflage. Berlin: Cornelsen Scriptor (siehe S. 173).

Mihăilescu, Preda, Axel Munk und Benjamin Tams (2009): *The Fuzzy Vault for Fingerprints is Vulnerable to Brute Force Attack*. In: *BIOSIG 2009. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Darmstadt, Germany, September 17-18*. Hrsg. von Arslan Brömme, Christoph Busch und Detlef Hühnlein. P-155. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag, S. 43–54. URL: http://subs.emis.de/LNI/Proceedings/Proceedings155/P-155.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 15).

Miller, Seth, Dustin Mixton und Jonathan Pickett (2004): *The UMAP Journal*. In: The UMAP Journal, 25 (3), hrsg. von Paul J. Campbell, S. 259. URL: http://eaton.math.rpi.edu/Faculty/Kramer/MCM/2004mcmsolutions.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 135).

Modi, Shimon K. (2011): *Biometrics in Identity Management*. Norwood: Artech House (siehe S. 92).

Moses, Kenneth R. (2011): *Automated Fingerprint Identification Systems (AFIS)*. In: *The Fingerprint Sourcebook*. Hrsg. von Alan McRoberts und Debbie McRoberts. U.S. Department of Justice, Office of Justice Programs. Kap. 6-1–6-33. URL: https://www.ncjrs.gov/pdffiles1/nij/225326.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 28).

Nuger, Kenneth P. und James L. Wayman (2005): *Biometrics and the US Constitution*. In: *Biometric Systems: technology, design and performance evaluation*. Hrsg. von James Wayman, Anil Jain, Davide Maltoni und Dario Maio. London: Springer London. Kap. Biometrics and the US Constitution, S. 311–333. DOI: 10.1007/1-84628-064-8_11 (siehe S. 156, 157).

Nuppeney, Markus (2007): *Biometrische Middleware basierend auf BioAPI 2.0*. In: *BIOSIG 2007: biometrics and electronic signatures. Proceedings of the special interest group on biometrics and electronic signatures,12th/13th Juliy 2007*. (Darmstadt, Germany). Hrsg. von Arslan Brömme, Christoph Busch und Detlef Hühnlein. Lecture Notes in Informatics (LNI). Gesellschaft für Informatik e. V. (GI). Darmstadt. URL: http://subs.emis.de/LNI/Proceedings/Proceedings108/gi-proc-108-010.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 69, 70).

o. V. (2005): *Fingerabdrücke nachmachen leichtgemacht*. In: Die Datenschleuder. Das wissenschaftliche Fachblatt für Datenreisende (87), hrsg. von CCC, Chaos Computer Club e.V., S. 14–16. URL: http://chaosradio.ccc.de/media/ds/ds087.pdf (letzter Abruf am: 01. 08. 2017) (siehe S. 15, 192).

o. V. (27. 11. 2007): *Fingerabdruck an der Supermarkt-Kasse genauso unsicher wie Biometrie im Reisepass*. Chaos Computer Club e. V. (online). URL: http://www.ccc.de/de/updates/2007/umsonst-im-supermarkt (letzter Abruf am: 01. 08. 2017) (siehe S. 15).

Orandi, Shahram, John Libert, John Grantham, Kenneth Ko, Stephen Wood, Frederick Byers, Bruce Bandini, Stephen Harvey und Michael Garris (2014): *Compression Guidance for 1000 ppi Friction Ridge Imagery*. NIST Special Publication 500-289. DOI: 10.6028/NIST.SP.500-289. URL: http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.500-289.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 55).

Ostap, Oleg (o. J.): *Presentation Preprocessing and Features Extraction Algorithm*. Slides. URL: http://fingerprintreco.cvs.sourceforge.net/viewvc/fingerprintreco/fingerprintreco/Documents/Presentations/Processing.pdf?revision=1.1 (letzter Abruf am: 02. 08. 2017) (siehe S. 127).

Ostap, Volodymyr (o. J.): *Matching Algorithm Presentation*. Slides. URL: http://fingerprintreco.cvs.sourceforge.net/viewvc/fingerprintreco/fingerprintreco/Documents/Presentations/Matching.pdf?revision=1.1 (letzter Abruf am: 02. 08. 2017) (siehe S. 127).

Pankanti, Sharath, Salil Prabhakar und Anil K. Jain (2002): *On the individuality of fingerprints*. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, 24 (8), S. 1010–1025. DOI: 10.1109/TPAMI.2002.1023799 (siehe S. 142).

Park, David (2017): *Brief Submitted on Behalf of the Innocence Network as Amicus Curiae in Support of Petitioner Glenn Ford. Glenn Ford v. Burl Cain*. No. 126, 005. URL: http://innocencenetwork.org/wp-content/uploads/2015/04/Ford-Glenn-v.-Cain.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 143).

Pato, Joseph N. und Lynette I. Millett, Hrsg. (2010): *Biometric Recognition. Challenges and Opportunities*. Washington, D.C.: The National Academies Press (siehe S. 102, 124, 151).

Patzelt, Werner J. (2007): *Einführung in die Politikwissenschaft*. 6., erw. u. neu bearb. Auflage. Passau: Wissenschaftsverlag Rothe (siehe S. 175, 176).

Pender, Jerome M. (21. 09. 2010): *FBI Next Generation Identification (NGI) Overview*. Biometric Consortium Conference Tampa, Florida September 21, 2010. Slides. URL: https://www.eff.org/files/pender-fbi-next-generation-identification-overview.pdf (letzter Abruf am: 04. 08. 2017) (siehe S. 170).

Penon, Johann und Siegfried Spolwig (1994): *Video-Center. Eine Fallstudie zur Einführung in relationale Datenbanken*. In: LOG IN, 14 (2), (siehe S. 199).

Penon, Johann und Siegfried Spolwig (1998): *Schöne visuelle Welt? Objektorientierte Programmierung mit DELPHI und JAVA*. In: LOG IN, 18 (5), URL: http://oszhandel.de/gymnasium/faecher/informatik/didaktik/delphi-java.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 199).

Petermann, Thomas und Arnold Sauter (2002): *Biometrische Identifikationssysteme. Sachstandsbericht*. Arbeitsbericht (76), Karlsruhe: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). URL: http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab076.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 124).

Petermann, Thomas, Constanze Scherz und Arnold Sauter (2003): *Biometrie und Ausweisdokumente. Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. Zweiter Sachstandsbericht*. Arbeitsbericht (93), Karlsruhe: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). URL: http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab093.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 124).

Ploeg, Irma van der (1999): *The illegal body: "Eurodac" and the politics of biometric identification*. In: Ethics and Information Technology, 1 (4), S. 295–302 (siehe S. 124).

Ploeg, Irma van der (2005): *The Machine-Readable Body*. Maastricht: Shaker Publishing (siehe S. 171).

Podio, Fernando L. und Fred Herr (2009): *Common Biometric Exchange Formats Framework Standardization*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil K. Jain. Berlin, Heidelberg: Springer Verlag, S. 183–189. DOI: 10.1007/978-0-387-73003-5_228 (siehe S. 72).

Prabhakar, Salil und Vance Bjorn (2008): *Biometrics in the Commercial Sector*. In: *Handbook of Biometrics*. Hrsg. von Anil K. Jain, Patrick Flynn und Arun A. Ross. New York: Springer Science+Business Media, S. 479–507 (siehe S. 154).

Pro Asyl (16. 12. 2009): *VG Hannover wirft Bundesamt für Migration und Flüchtlinge Verfassungsbruch vor*. Pro Asyl (online). URL: https://www.proasyl.de/pressemitteilung/vg-hannover-wirft-bundesamt-fuer-migration-und-fluechtlinge-verfassungsbruch-vor/ (letzter Abruf am: 02. 08. 2017) (siehe S. 193).

Putte, Ton van der und Jeroen Keuning (2000): *Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned*. In: *Proceedings of the IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, CARDIS 2000, September 20-22, 2000, Bristol, UK*. 52. Kluwer Academic Publishers, S. 289–303. DOI: 10.1007/978-0-387-35528-3_17. URL: http://cryptome.org/fake-prints.htm (letzter Abruf am: 02. 08. 2017) (siehe S. 15).

Rebera, Andrew P. und Barry Guihen (2017): *Biometrics for an ageing society societal and ethical factors in biometrics and ageing*. In: *BIOSIG 2012. Proceedings of the 11th International Conference of the Biometrics Special Interest Group, September 6-7 in Darmstadt, Germany*. Hrsg. von Arslan Brömme und Christoph Busch. P-196. Gesellschaft für Informatik e. V. (GI). Bonn: Köllen Verlag, S. 1–4. URL: https://subs.emis.de/LNI/Proceedings/Proceedings196/409.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 140).

Rieger, Frank (21. 09. 2013): *Chaos Computer Club hackt Apple TouchID*. Chaos Computer Club e. V. (online). URL: http://www.ccc.de/de/updates/2013/ccc-breaks-apple-touchid (letzter Abruf am: 03. 08. 2017) (siehe S. 15).

Robben, Bernard und Heidi Schelhowe, Hrsg. (2012): *Be-greifbare Interaktionen*. Bielefeld: transcript Verlag (siehe S. 22).

Roberts, Chris (2007): *Biometric attack vectors and defences*. In: Computers & Security, 26 (1), S. 14–25. DOI: 10.1016/j.cose.2006.12.008 (siehe S. 114, 115).

Roethenbaugh, Gary (1998): *ICSA Biometrics Industry Guide. Biometrics Explained*. URL: https://web.archive.org/web/19980529094811/http://www.icsa.net/services/consortia/cbdc/explained.htm (letzter Abruf am: 03. 08. 2017) (siehe S. 33, 140, 151, 153–156).

Röhner, Gerhard, Torsten Brinda, Volker Denke, Lutz Hellmig, Theo Heußer, Arno Pasternak, Andreas Schwill und Monika Seiffert (2016): *Bildungsstandards Informatik für die Sekundarstufe II*. In: LOG IN, 36 (183/184), hrsg. von Arbeitskreis »Bildungsstandards SII« des Fachausschusses »Informatische Bildung in Schulen« (FA IBS) und der Fachgruppe »Didaktik der Informatik« (FG DDI). URL: https://www.gi.de/fileadmin/redaktion/empfehlungen/Bildungsstandards-Informatik-SekII.pdf (letzter Abruf am: 31. 07. 2017) (siehe S. 182–185).

Romandetti, Kristin (2004): *Recognizing and Responding to a Problem with the Admissibility of Fingerprint Evidence under Daubert*. In: Jurimetrics, 45 (1), S. 41–58. URL: http://www.jstor.org/stable/29762878 (siehe S. 142).

Rosenfeld, Azriel und Harry Wechsler (2000): *Pattern recognition: Historical perspective and future directions*. In: International Journal of Imaging Systems and Technology, 11 (2), S. 101–116. DOI: 10.1002/1098-1098(2000)11:2<101::AID-IMA1>3.0.CO;2-J (siehe S. 41–43, 67).

Ross, Arun A., Karthik Nandakumar und Anil K. Jain (2006): *Handbook of Multibiometrics*. International Series on Biometrics. New York: Springer US. DOI: 10.1007/0-387-33123-9 (siehe S. 34).

Ryu, Choonwoo, Seong G. Kong und Hakil Kim (2011): *Enhancement of feature extraction for low-quality fingerprint images using stochastic resonance*. In: Pattern Recognition Letters, 32 (2), S. 107–113. DOI: 10.1016/j.patrec.2010.09.008 (siehe S. 141).

Sammons, Brent (02. 03. 2015): *Breakthrough 3D fingerprint authentication with Snapdragon Sense ID | Qualcomm*. Qualcomm – OnQ Blog. URL: https://www.qualcomm.com/news/snapdragon/2015/03/02/breakthrough-3d-fingerprint-authentication-snapdragon-sense-id (letzter Abruf am: 03. 08. 2017) (siehe S. 53).

Scheck, Barry C., Peter J. Neufeld und Elaine Metlin (11. 04. 2005): *Brief amicus curiae of Innocence Project. Bobby Lee Holmes versus the State of South Carolina*. No. 04-1327. URL: http://innocencenetwork.org/wp-content/uploads/2015/04/Holmes-v.-South-Carolina.pdf (letzter Abruf am: 03. 08. 2017) (siehe S. 143).

Schelhowe, Heidi (2012): *Interaktionsdesign für reflexive Erfahrung. Digitale Medien für Bildung*. In: *Be-greifbare Interaktionen. Der allgegenwärtige Computer: Touchscreens, Wearables, Tangibles und Ubiquitous Computing*. Hrsg. von Bernard Robben und Heidi Schelhowe. Bielefeld: transcript Verlag, S. 253–272 (siehe S. 179, 180, 222).

Scheuermann, Ulrike (2013): *Schreibdenken: Schreiben als Denk- und Lernwerkzeug nutzen und vermitteln*. Opladen, Toronto: Verlag Barbara Budrich / UTB (siehe S. 217).

Schlingloff, Bernd-Holger (2006): *Softwarequalität — Geschichte und Trends*. In: *Informatik: Aktuelle Themen im historischen Kontext*. Hrsg. von Wolfgang Reisig und Johann-Christoph Freytag. Berlin, Heidelberg: Springer-Verlag, S. 329–345. DOI: 10.1007/3-540-32743-6_14 (siehe S. 79).

Schmelzer, André und Christian Steinfeldt (02. 11. 2012): *Fingerabdrücke Hacken*. Folien. URL: http://waste.informatik.hu-berlin.de/Lehre/ws1213/SE_FingerIdent/01112012/011112_hacking_fingers_folien.pdf (letzter Abruf am: 30. 07. 2017) (siehe S. 220).

Schneider, John K., Jack C. Kitchens und James T. Baker (2013): *Ultrasonic fingerprint scanning using a plane wave*. Version US Patent 8,601,876. URL: http://www.google.com/patents/US8601876 (letzter Abruf am: 03. 08. 2017) (siehe S. 53).

Schubert, Sigrid und Andreas Schwill (2011): *Didaktik der Informatik*. 2. Auflage. Heidelberg: Spektrum Akademischer Verlag (siehe S. 173).

Schuckers, Stephanie (02. 03. 2016): *Presentations and Attacks, and Spoofs, Oh My*. In: Image and Vision Computing, 55 (1), S. 26–30. URL: https://www.clarkson.edu/biosal/pdf/Presentations%20and%20Attacks.pdf (letzter Abruf am: 02. 08. 2017) (siehe S. 118).

Setlak, Dale R. (2004): *Advances in Fingerprint Sensors Using RF Imaging Techniques*. In: *Automatic Fingerprint Recognition Systems*. Hrsg. von Nalini Ratha und Ruud Bolle. New York: Springer New York, S. 27–53. DOI: 10.1007/0-387-21685-5_2 (siehe S. 45, 50–52, 106, 109, 168, 170).

Setlak, Dale R. (2009): *Biometric Sample Acquisition*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil K. Jain. Berlin, Heidelberg: Springer Verlag, S. 96–101. DOI: 10.1007/978-0-387-73003-5_212 (siehe S. 43, 49, 50, 53, 54).

Siefkes, Dirk, Peter Eulenhöfer, Heike Stach und Klaus Städtler, Hrsg. (1998): *Sozialgeschichte der Informatik*. Studien zur Wissenschafts- und Technikforschung. Wiesbaden: Deutscher Universitätsverlag (siehe S. 19).

Simon, Taryn, Peter Neufeld und Barry Scheck (2003): *The Innocents*. New York: Umbrage (siehe S. 142).

Spychiger, Maria B. (2008): *Lernen aus Fehlern und Entwicklung von Fehlerkultur*. In: Erwägen Wissen Ethik, 19 (3), S. 274–282 (siehe S. 177).

starbug (09. 10. 2004): *Wie können Fingerabdrücke nachgebildet werden?* Chaos Computer Club e. V. (online). URL: http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren.de (letzter Abruf am: 03. 08. 2017) (siehe S. 15, 192).

Steria Group Press Office (14. 01. 2003): *The European Commission chooses Steria's biometrics know-how to process asylum requests and fight illegal immigration*. Press Release. URL: https://web.archive.org/web/20031214123703/http://www.steria.com/press/down/0114_Eurodac_eng.pdf (letzter Abruf am: 03. 08. 2017) (siehe S. 13).

Stigler, Stephen M. (2000): *The Problematic Unity of Biometrics*. In: Biometrics, 56 (3), S. 653–658. URL: http://www.jstor.org/stable/2676905 (siehe S. 25, 27, 32).

Stoney, David A. und John I. Thornton (1986): *A critical analysis of quantitative fingerprint individuality models*. In: Journal of Forensic Science, 31 (4), S. 1187–1216 (siehe S. 135).

TABULA RASA (2013-2014): *TABULA RASA*. You-Tube-Kanal. URL: https://www.youtube.com/channel/UCoHA9lGDrtEUim_mdtPwQ6w (letzter Abruf am: 03. 08. 2017) (siehe S. 15).

Tassabehji, Rana und Mumtaz A. Kamala (2012): *Evaluating biometrics for online banking: The case for usability*. In: International Journal of Information Management, 32 (5), S. 489–494. DOI: 10.1016/j.ijinfomgt.2012.07.001 (siehe S. 35).

TeleTrusT e. V. (2015): *Jahresbericht 2014*. TeleTrusT e. V. URL: https://www.teletrust.de/fileadmin/docs/jahresbericht/TeleTrusT-Jahresbericht_2014.pdf (letzter Abruf am: 03. 08. 2017) (siehe S. 165).

Thieme, Michael (11. 11. 2009): *International Biometric Group Announces the Availability of the Biometrics Market and Industry Report 2009-2014*. PRWeb (online). URL: http://www.prweb.com/releases/2009/11/prweb3188664.htm (letzter Abruf am: 02. 08. 2017) (siehe S. 169).

Tian, Jie, Yangyang Zhang und Kai Cao (2009): *Fingerprint Matching, Automatic*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil K. Jain. Boston, MA: Springer US. Kap. Fingerprint Matching, Automatic, S. 497–502. DOI: 10.1007/978-0-387-73003-5_54 (siehe S. 49).

Tilton, Catherine J. (2009): *Biometric Interfaces*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil K. Jain. Berlin, Heidelberg: Springer Verlag, S. 90–95. DOI: 10.1007/978-0-387-73003-5_185 (siehe S. 68, 69).

Tilton, Catherine J. (2011): *Standards – Getting Started*. Planet Biometrics (online). URL: http://www.planetbiometrics.com/creo_files/upload/article-files/getting_started_-_biometric_standards_-_v2_(sep2011).pdf (letzter Abruf am: 29. 07. 2017) (siehe S. 164).

Töpfer, Eric (2015): *Ein Ding, sie zu finden… Eurodac und die biometrische Erfassung asylsuchender und irregulärer Migranten*. In: DANA – Datenschutznachrichten, (2), *Datenerfassung und Flüchtlinge*, S. 64–68. URL: http://www.emato.de/wp-content/uploads/2016/08/Toepfer-2015-Eurodac.pdf (letzter Abruf am: 10. 01. 2017) (siehe S. 103).

Vanderkolk, John R. (2011): *The Fingerprint Sourcebook*. In: *The Fingerprint Sourcebook*. Hrsg. von Alan McRoberts und Debbie McRoberts. U.S. Department of Justice, Office of Justice Programs, S. 9-1–9-26. URL: http://www.nij.gov/publications/pages/publication-detail.aspx?ncjnumber=225320 (letzter Abruf am: 02. 08. 2017) (siehe S. 28, 31).

Važan, Robert (05. 09. 2012a): *Building Awesome Opensource Projects | SourceAFIS*. Robert's blog (online). URL: http://www.sourceafis.org/blog/how-to-build-awesome-opensource-projects/ (letzter Abruf am: 28. 07. 2017) (siehe S. 126).

Važan, Robert (01. 10. 2012b): *SourceAFIS 1.7 | SourceAFIS*. SourceAFIS-Blog (online). URL: https://web.archive.org/web/20170409002811/http://www.sourceafis.org/blog/sourceafis-1-7/ (letzter Abruf am: 28. 07. 2017) (siehe S. 127, 128).

Važan, Robert (23. 05. 2013a): *SourceAFIS / Discussion / Open Discussion: Humble beginnings*. SourceAFIS-Discussion-Forum (online). URL: http://sourceforge.net/p/sourceafis/discussion/1051112/thread/5578823c/?limit=25%5C#7348 (letzter Abruf am: 28. 07. 2017) (siehe S. 127).

Važan, Robert (12. 06. 2013b): *SourceAFIS / Tutorial*. SourceAFIS-Wiki (online). URL: https://en.wikibooks.org/wiki/SourceAFIS/Tutorial (letzter Abruf am: 28. 07. 2017) (siehe S. 128).

Važan, Robert (27. 11. 2014): *SourceAFIS / Discussion / Open Discussion: Good book on fingerprint recognition?* SourceAFIS-Discussion-Forum (online). URL: http://sourceforge.net/p/sourceafis/discussion/1051112/thread/1afc1c5e/ (letzter Abruf am: 28. 07. 2017) (siehe S. 127).

Vec, Miloš (2001): *Die Spur des Täters. Bertillonage, Daktyloskopie und Jodogramm: Fortschritte und Versprechungen der naturwissenschaftlichen Kriminalistik um 1900*. In: juridikum. zeitschrift im rechtsstaat, 2, S. 89–94. URL: http://www.rg.mpg.de/686694/vec_juridikum.pdf (letzter Abruf am: 03. 08. 2017) (siehe S. 26, 27).

Waggett, Peter (2015): *Experiences from Large Scale Testing of Systems using Biometric Technologies*. Report (27190 EN), European Reference Network for Critical Infrastructure Protection/EU JRC (siehe S. 160).

Wasserman, Philip D. (26. 12. 2005): *Solid-State Fingerprint Scanners. A Survey of Technologies*. National Institute of Standards und Technology (NIST). URL: https://www.nist.gov/sites/default/files/documents/2016/12/21/ssfs_113005.pdf (letzter Abruf am: 03. 08. 2017) (siehe S. 104).

Watson, Blair (2010): *Biometric Passports. How Secure Are They?* In: FrontLine Security, 5 (2), URL: http://security.frontline.online/article/2010/2/2598-Biometric-Passports- (letzter Abruf am: 03. 08. 2017) (siehe S. 15).

Watson, Craig I., Michael D. Garris, Elham Tabassi, Charles L. Wilson, R. Michael McCabe, Stanley Janet und Kenneth Ko (2007a): *User's Guide to Export Controlled Distribution of NIST Biometric Image Software (NBIS-EC)*. NIST Interagency/Internal Report (NISTIR) - 7391. National Institute of Standards und Technology. URL: https://www.nist.gov/publications/users-guide-export-controlled-distribution-nist-biometric-image-software-nbis-ec (letzter Abruf am: 03. 08. 2017) (siehe S. 127).

Watson, Craig I., Michael D. Garris, Elham Tabassi, Charles L. Wilson, R. Michael McCabe, Stanley Janet und Kenneth Ko (2007b): *User's Guide to NIST Biometric Image Software (NBIS)*. NIST Interagency/Internal Report (NISTIR) - 7392. National Institute of Standards und Technology. URL: https://www.nist.gov/publications/users-guide-nist-biometric-image-software-nbis (letzter Abruf am: 03. 08. 2017) (siehe S. 127).

Wayman, James L. (1998): *A Definition of "Biometric"*. In: *National Biometric Test Center Collected Works 1997-2000*. Hrsg. von James L. Wayman. Version 1.3, S. 21–23. URL: https://pdfs.semanticscholar.org/7532/d081429b083c5f920adf3559ba0d857447b2.pdf (letzter Abruf am: 03. 08. 2017) (siehe S. 120, 122, 157).

Wayman, James L., Hrsg. (2000): *National Biometric Test Center Collected Works 1997-2000*. Version 1.3. URL: https://pdfs.semanticscholar.org/7532/d081429b083c5f920adf3559ba0d857447b2.pdf (letzter Abruf am: 03. 08. 2017) (siehe S. 144, 164).

Wayman, James L. (2004): *Multifinger Penetration Rate and ROC Variability for Automatic Fingerprint Identification Systems*. In: *Automatic Fingerprint Recognition Systems*. Hrsg. von Nalini Ratha und Ruud Bolle. New York: Springer, S. 305–316. DOI: 10.1007/0-387-21685-5_15 (siehe S. 117).

Wayman, James L. (2005): *An Introduction to Biometric Authentication Systems*. In: *Biometric Systems: technology, design and performance evaluation*. Hrsg. von James L. Wayman, Anil K. Jain, Davide Maltoni und Dario Maio. London, Berlin und Heidelberg: Springer-Verlag, S. 1–20 (siehe S. 36, 87, 144).

Wayman, James L. (16. 09. 2013): *Special "Tutorial" on "Biometrics"*. URL: http://biometrics.org/bc2013/presentations/special_tutorial_bcc_2013.pdf (letzter Abruf am: 25. 08. 2014) (siehe S. 78, 102, 120).

Wayman, James L., Anil K. Jain, Davide Maltoni und Dario Maio, Hrsg. (2005): *Biometric Systems: technology, design and performance evaluation*. London, Berlin und Heidelberg: Springer-Verlag (siehe S. 37, 110, 148, 149).

Wayman, James L., Rene McIver, Peter Waggett, Stephen Clarke, Masanori Mizoguchi, Christoph Busch, Nicolas Delvaux und Andrey Zudenkov (2014): *Vocabulary harmonisation for biometrics: the development of ISO/IEC 2382 Part 37*. In: IET Biometrics, 3 (1), 1–8(7). DOI: 10.1049/iet-bmt.2013.0003 (siehe S. 37, 119, 122, 148).

Weihmann, Robert (2009): *Kriminaltechnik. Expertise für Fraunhofer Institut für Naturwissenschaftlich-Technische Trendanalyse (INT)*. Robert Weihmann – Kriminalistik (online). URL: http://www.weihmann.info/images/Aufsaetze/16%20Expertise%20Kriminaltechnik.pdf (letzter Abruf am: 03. 08. 2017) (siehe S. 31).

Weingardt, Martin (2004): *Fehler zeichnen uns aus*. Bad Heilbrunn: Julius Klinkhardt (siehe S. 72, 73, 79, 130, 131).

Weiß, Christel (20. 06. 2005): *Entwicklung der Medizinischen Statistik in Deutschland – der lange Weg dahin*. In: GMS Medizinische Informatik, Biometrie und Epidemiologie, 1 (2), Doc12. URL: http://www.egms.de/static/de/journals/mibe/2005-1/mibe000012.shtml (letzter Abruf am: 03. 08. 2018) (siehe S. 26).

Wendt, Norbert (o. J.): *»Hasenjagd auf hoher See«. Populäre Irrtümer über Gesichtserkennung*. Unveröffentlichte Vortragsfolien. L-1 Identity Solutions (siehe S. 102, 103).

Wiedemann, Ursula (2012): *Biometrie – Stand und Chancen der Vermessung des Menschen*. Kulturen – Kommunikation – Kontakte. Berlin: Frank & Timme GmbH (siehe S. 167).

Wiggin, Phillip und Lars Ericson (2014): *Contactless Fingerprint Technologies Assessment*. Report. Version 2. National Institute of Justice (NIJ), Sensor, Surveillance, und Biometric Technologies (SSBT), Center of Excellence (CoE). URL: https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf (letzter Abruf am: 03. 08. 2018) (siehe S. 51).

Winograd, Terry und Fernando Flores (1992): *Erkenntnis Maschinen Verstehen*. 2. Auflage (1989). Berlin: Rotbuch Verlag (siehe S. 166, 180).

Witten, Helmut, Johann Penon und Alexander Dietz (2006): *SOL – Schule ohne Lehrer?* In: LOG IN, 26 (138/139), S. 74–81 (siehe S. 199).

Xueyan, Li und Guo Shuxu (2008): *The Fourth Biometric-Vein Recognition*. In: *Pattern recognition techniques, technology and applications*. Hrsg. von Peng-Yeng Yin. INTECH Open Access Publisher, S. 537–546. URL: http://cdn.intechopen.com/pdfs/5801/InTech-The_fourth_biometric_vein_recognition.pdf (letzter Abruf am: 03. 08. 2017) (siehe S. 169).

Yau, Wei-Yun (2009): *Fingerprint Templates*. In: *Encyclopedia of Biometrics*. Hrsg. von Stan Z. Li und Anil Jain. Boston, MA: Springer US, S. 523–528. DOI: 10.1007/978-0-387-73003-5_51 (siehe S. 154).

Yau, Wei-Yun, Zujun Hou, Vutipong Areekul und Suksan Jirachaweng (2013): *Fingerprint Recognition*. In: *Biometrics. From Fiction to Practice*. Hrsg. von Eliza Yingzi Du. Singapore: Pan Stanford Publishing, S. 11–28 (siehe S. 49, 57, 59, 60).

Zhou, Zhijian, Man Wong und Libor Rufer (2010): *The Design, Fabrication and Characterization of a Piezoresistive Tactile Sensor for Fingerprint Sensing*. In: *2010 IEEE Sensors*. Kona, HI, S. 2589–2592. DOI: 10.1109/ICSENS.2010.5690176 (siehe S. 53).

Rechtliche Quellen

95/46/EC (23. 11. 1995): *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=DE (letzter Abruf am: 03. 08. 2017) (siehe S. 38).

95/46/EG (23. 11. 1995): *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML (letzter Abruf am: 03. 08. 2017) (siehe S. 38).

BVerfG 502/09 (30. 12. 2012): *Beschluss der 1. Kammer des Ersten Senats vom 30. Dezember 2012 in dem Verfahren über die Verfassungsbeschwerde Juli Zeh/Frank Selbmann gegen §4 Abs. 3 und §4 Abs. 4 des Passgesetzes vom 19. April 1986 (BGBl I S. 537) in der Fassung vom 20. Juli 2007 (BGBl I S. 1566)*. BVerfG, 1 BvR 502/09 vom 30.12.2012, Absatz-Nr. (1 - 10). URL: http://www.bverfg.de/entscheidungen/rk20121230_1bvr050209.html (letzter Abruf am: 03. 08. 2017) (siehe S. 14).

EU-DSGVO (04. 05. 2016): *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).* URL: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.DEU&toc=OJ:L:2016:119:TOC (letzter Abruf am: 20. 07. 2017) (siehe S. 38).

EU GDPR (03. 08. 2017): *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (letzter Abruf am: 20. 07. 2017) (siehe S. 38).

EuGH C-291/12 (20. 06. 2013): *Urteil des Gerichtshofes (Vierte Kammer) vom 17. Oktober 2013. Michael Schwarz gegen Stadt Bochum.* Urteil. EuGH, Urteil vom 17. 10. 1013, Rs. C-291/12. URL: http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0291&lang1=de&type=TXT&ancre= (letzter Abruf am: 03. 08. 2017) (siehe S. 14).

VO EG 2252/2004 (29. 12. 2004): *Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten.* URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:DE:PDF (letzter Abruf am: 03. 08. 2017) (siehe S. 14).

VO EG 2725/2000 (11. 12. 2000): *Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Errichtung von „Eurodac" für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Umsetzung des Dubliner Übereinkommens.* URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000R2725:DE:NOT (letzter Abruf am: 03. 08. 2017) (siehe S. 13).

VO EG 767/2008 (09. 07. 2008): *Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung).* URL: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32008R0767&from=DE (letzter Abruf am: 03. 08. 2017) (siehe S. 14).

Gesprächsnotizen, Protokolle

Knaut, Andrea (16. 12. 2014): *Eigene Notizen zur Sitzung der TeleTrusT-AG Biometrie.* Bundesdruckerei, Berlin: TeleTrusT e. V. (siehe S. 15).

Knaut, Andrea (03. 02. 2015): *Notizen zum Gespräch mit Dr. Elke Dallmer, Bereich Biometrie-Zertifizierung, Security Research & Consulting GmbH* (siehe S. 15).

Danksagung

An erster Stelle bedanke ich mich bei Wolfgang Coy für die Möglichkeit, diese Arbeit im akademischen Rahmen schreiben zu können. Die Zeit bei IBuG hat mir wichtigen intellektuellen Austausch und den hilfreichen Zugriff auf viele Ressourcen des Wissenschaftsbetriebs ermöglicht.

Ein großer Dank gilt auch allen Teilnehmenden meiner Workshops, Seminare und Unterrichtsstunden für die vielen tollen Ideen und Diskussionen. Veronika Oechtering und Thomas Lingens danke ich hierbei besonders für die Gelegenheiten, die Projektkurse für diese Arbeit auf der Informatica Feminale in Bremen bzw. am OSZ Handel I in Berlin durchführen zu können.

Für das Gegenlesen der Korrekturfassungen einzelner Kapitel und viele hilfreiche Fragen und Kommentare möchte ich Katja Grote, Tobias Jaecker, Rebekka Ladewig, Magdalena Soyka, Rebekka Streck und Alexander Weiß sehr danken. Ein spezieller Dank gilt Agata Królikowski, die schon sehr frühe Fassungen meiner Arbeit kommentiert hat und mit der ich oft produktiv über das gesamte Projekt gesprochen habe.

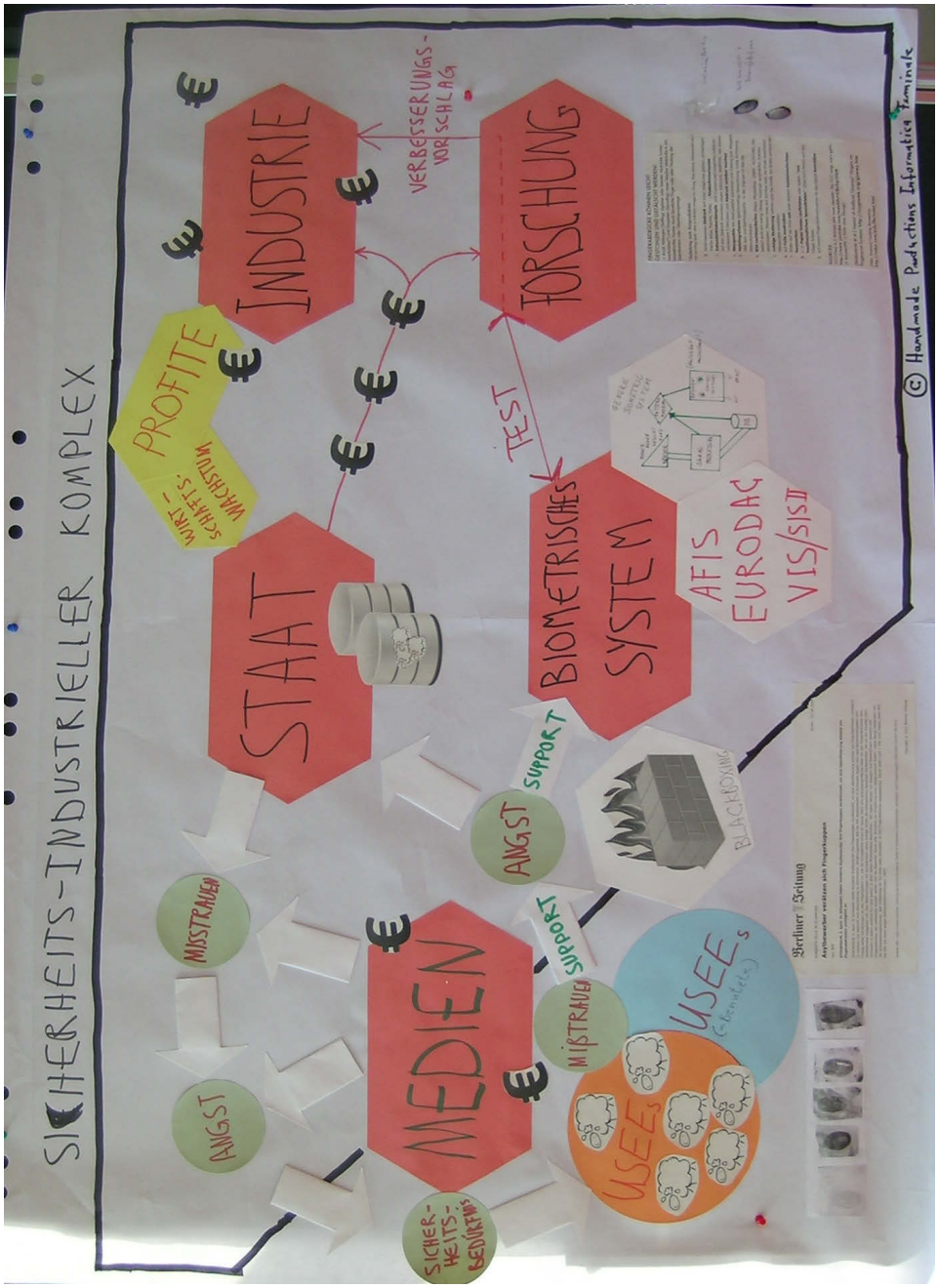
Sandra Fuhrmann danke ich für die aufbauenden Begleitgespräche und ihren Pragmatismus.

Ein sehr persönlicher Dank geht an Steve Pracanin für die moralische Unterstützung, das Zuhören und das Vertrauen.

Andrea Knaut, Berlin, 15. August 2017

Anhang

Plakat »Sicherheits-industrieller Komplex«, Informatica Feminale



Anhang

Eingereichtes Unterrichtskonzept OSZ Handel I

Unterrichtsprojekt „Überwachungstechnologie begreifen: Wa(h)re Identität und der Fingerabdruck.“

Andrea Knaut

14. September 2012

[Entwurf, v 0.2]

Motivation

Das folgende Projektkonzept wird als Teil meiner Dissertation über die *Fehlertransparenz biometrischer Systeme* entwickelt, ausprobiert, entwickelt und ausgewertet. Angeregt ist die Herangehensweise an mein Thema über ein Bildungsprojekt durch meine Arbeit im Bereich der Fachdidaktik der Informatik und viele Gespräche mit Lehrer_innen, meinem Doktorvater und sonstigen geduldigen Kritiker_innen eines solchen Forschungsvorhabens.

Der Entwurf umfasst modular angelegte Lehr- und Lernbausteine, die ein kritisches Verstehen der Funktionalität und den Fehlern einer Kontrolltechnologie wie einem biometrischen Fingerabdruckidentifizierungssystem ermöglichen sollen. Konkret werden diese Lernbausteine an den Konzepten der Initiative *Informatik im Kontext* orientiert und zunächst für die projektorientierte Arbeit in der Schule oder der außerschulischen Bildungsarbeit ab einem Alter von 14 Jahren entworfen. Das didaktische Konzept soll zusätzlich zur Lebensweltorientierung des IniK-Ansatzes vor allem das kritisch-hinterfragende Denken bezüglich der vielschichtigen Fehler motivieren, die in vermeintlich nach klaren, standardisierten Formaten, Testmethoden und Modellierungen entwickelten Maschinen oft verschleiert sind oder einer Fehlbenutzung zugeschrieben werden. Das bedeutet einerseits, die Übersetzung der formalisierten statististischen Fehlerkonzepte in ihre konkrete soziale Bedeutung aus vielerlei Perspektive und die ihnen zugrunde liegenden formalen Vereinfachungen hinsichtlich der Konzepte menschlicher Identität und Kommunikation zu versuchen (!), andererseits, speziell die gesellschaftliche Funktion und strukturelle Einbettung rechnergestützter Überwachungstechnologien in politische, ökonomische oder kulturelle Institutionen zu analysieren und die Bedeutung der kanonisierten und nicht kanonisierbaren Fehler dieser Technologien sowohl auf menschlicher als auch auf technischer Ebene in den Vordergrund zu rücken – insbesondere Methoden der sogenannten *Surveillance Studies* sollen dabei in die Konzeptionierung der Lernanregungen einfließen.

Worum geht es?

In der für 18 Unterrichtsstunden geplanten Einheit können sich die Schüler_innen mit dem Einsatz von Rechentechnik im Bereich der Personenidentifikation, der Biometrie, praktisch auseinandersetzen. Die Erfassung von Fingerabdrücken und Passbildern als biometrische Daten auf RFID-Chips in Reisepässen oder in großen Datenbanken ist inzwischen weltweit eine normale Prozedur geworden. Auch in geschäftlichen oder privaten Kontexten werden digitale Muster verschiedener Körpermerkmale vielfältig genutzt. In Europa hat die Nutzung biometrischer Daten ihre längste Tradition in der Kriminaltechnik. In kaum einem Kriminalroman oder -film fehlen Fingerabdrücke zur Suche nach der/dem Täter_in. Inzwischen natürlich mit Hilfe der sogenannten Automatisierten Fingerabdruck-Identifizierungs-Systeme (AFIS).

Eingereichtes Unterrichtskonzept OSZ Handel I

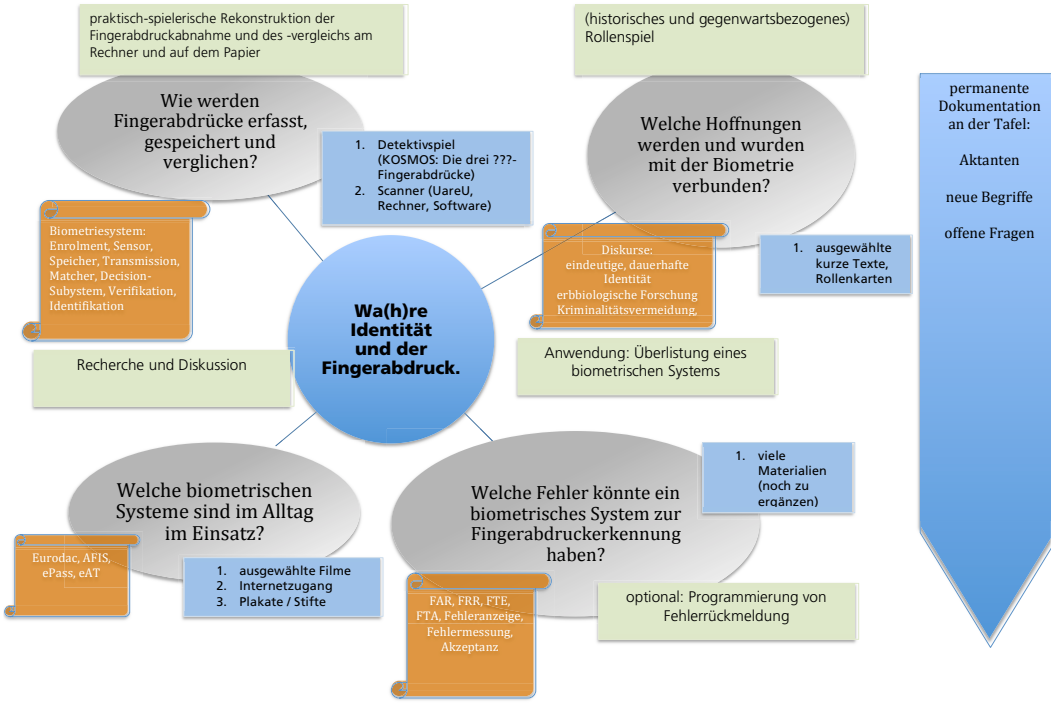
In biometrischen Systemen ist es nicht oder nur sehr eingeschränkt möglich von außen nachzuvollziehen, wie und wie korrekt sie funktionieren. Letztlich weiß nur die/der Betroffene und Leute, die sie oder ihn kennen, ob ein solches System sie richtig erkannt hat oder nicht. Aber wem lässt sich unter welchen Umständen einfacher vertrauen? Was heißt eigentlich dieses Kennen oder Erkennen? Nicht zuletzt diesen schwierigen Fragen soll sich die Unterrichtsreihe spielerisch, entdeckend und kontrovers annähern. Angst und falscher Respekt vor vermeintlich perfekten Kontrollsystemen sollen abgebaut werden. Dazu soll analysiert werden, wie ein solches System modelliert und konkret implementiert ist, welche Aspekte der Signalverarbeitung und der Mustererkennung eine wichtige Rolle spielen und welche Fehler sich technisch zwangsläufig immer ergeben und inwiefern der/die Person, die das System nutzen muss, überhaupt davon erfährt. Außerdem soll klarer werden, dass biometrische Systeme Teil von aus bestimmten Gründen in soziale und historische Kontexte eingebetteten Überwachungstechnologien sind, die nie losgelöst von bestimmten Grundannahmen über menschliche Identität und Interessen vieler verschiedener Akteure aus Staat oder Privatwirtschaft sind.

Berührte Standards und Kompetenzen

Die Informatik als Wissenschaft der Verarbeitung von Daten, die als Informationen mannigfache Bedeutung haben, bietet zahlreiche Werkzeuge zur Verwirklichung strukturierter Überwachung von Individuen. Die kritische *Beurteilung der Wechselwirkungen zwischen Informatiksystemen, Mensch und Gesellschaft* ist daher ein wichtiger Bestandteil der Informatikausbildung bereits an der Schule und soll in dieser Reihe das zentrale Gewicht haben. Zur Erarbeitung der *zentralen Begriffe, Modelle und Algorithmen*, die in einem biometrischen System verwendet werden, werden die alten Verfahren des Fingerabdruckabgleichs mit Papier und Druckerschwärze praktisch nachvollzogen. Ein weiterer informatischer Schwerpunkt liegt auf der *Fehleranalyse und Test* der Überwindungssicherheit eines ausgewählten Systems. Hier bieten sich Anknüpfungspunkte für beispielhaft implementierte Fehlervisualisierungen (eine optionale Erweiterung der Reihe allerdings). An die Betrachtung der Fehler eines Biometriesystems knüpft sich nahtlos die *Frage der Akzeptanz* und der Probleme desselben an – hier werden sowohl historische, aber auch aktuelle politische Debatten in ein *Rollenspiel* einfließen, um Konzepte von Identität und Vertrauen in ihrer Vielfältigkeit zu erschließen und die Problematik der Formalisierung und Entkontextualisierung einer maschinellen Identifikation zu verstehen. Schließlich werden die *Akteure mit ihren verschiedenen Interessen und Aussagen* beim Einsatz biometrischer Systeme in ihren Beziehungen auf Plakaten, die begleitend zur Recherche im Netz, dargestellt. Die Ergebnisse dieser Arbeit, die in gewisser Weise eine Visualisierung eines Diskurses rund um die Biometrie ist, können *gemeinsam bewertet und kontrovers diskutiert* werden.

Eingereichtes Unterrichtskonzept OSZ Handel I

Die geplanten Module und ein möglicher Ablauf



Auf dem Schaubild sind die Hauptfragestellungen der vier großen inhaltlichen Bausteine in grauen Ellipsen dargstellt. In den blauen Kästen finden sich erste Hinweise für benötigtes Material. Wichtige inhaltliche Begriffe, die erarbeitet werden sollen, sind in den orangenen Kästen aufgeführt und in grün sind sehr grob methodische Herangehensweisen genannt. Die Festlegung auf konkrete Formen der Diskussion bspw. als offen, Fish-Bowl oder Gruppenpuzzle oder auf Einzel- oder Gruppenarbeit wird in der Detailplanung der Module vorgeschlagen. Die Anordnung der Bausteine ist im Grunde flexibel und könnte auch verzahnt werden. Während der gesamten Reihe sollten zentrale Begriffe, Akteure, aber auch nicht schnell zu klärende inhaltliche Nachfragen an der Tafel, auf Plakaten oder in einem Wiki diskutiert werden.

Eine erste Abschätzung des Zeitaufwands und ein möglicher Vorschlag für eine Reihenfolge der Module wird in der folgenden Tabelle vorgenommen. Die Stundenzahlen meinen auf 45-minütige Schulstunden:

Leitfrage eines Moduls	*geschätzte Dauer*	*grober methodischer Ansatz*	*Arbeitsmaterialien*
I. Wie werden Fingerabdrücke erfasst, gespeichert und verglichen?	4h	praktische Rekonstruktion alter und neuen Methoden in Zweier- bis Dreiergruppen, für den Erfahrungsaustausch u. U. Gruppenpuzzle o. Schülerpräsentation	je nach Klassengröße (max. 20 Leute): 1 Rechner mit Fingerabdruckscanner ink. Software pro Gruppe (max. 5x) 1 Detektivset pro Gruppe (max. 5x), Doku-Plakate und Stifte

Eingereichtes Unterrichtskonzept OSZ Handel I

Leitfrage eines Moduls	*geschätzte Dauer*	*grober methodischer Ansatz*	*Arbeitsmaterialien*
II. Welche Hoffnungen werden und wurden mit der Biometrie verbunden?	3h	(historisches und gegenwartsbezogenes) Rollenspiel	Rollenkarten, ausgewählte Texte (Arbeitsblätter oder digitale Vorlagen)
III. Welche Fehler könnte ein biometrisches System zur Fingerabdruckerkennung haben?	8h	Anwendung: Überlistung eines biometrischen Systems in Dreier- bis Vierergruppen	Holzleim, Schnellkleber, Graphitpulver, Pinsel, Digitalkamera, Drucker, bedruckbare Folien, Gläser, Rechner
IV. Welche technischen und sozialen Akteure sind an derzeitig aktiven biometrischen Systemen beteiligt?	2h	Recherche und Diskussion	
optional IIIb: Welche Visualisierungen der Fehler am UserInterface implementieren?	4h	Programmierung von Fehlerrückmeldungen der Biometrie-Software	Developer-Kit Fingerabdrucksoftware, Tutorials, Entwicklungs- und Testumgebung
optional IVb: Exkursion oder Einladung zu einem/eines Hersteller(s), Beamten, Betroffenen, o.ä.	2h (a) Tag Exk. (b) 1h (c) 2h (d)	(a) Vorbereitung von Interviewsfragebögen, (b) Exkursion ODER (c) Besuch, (d) Auswertung	

Anhang

Klausuraufgabe OSZ Handel

2. Klausur im Fach Wirtschaftsinformatik	
Name:	19.11.2012

Aufgabe 1 ..... [6 P/]

Grundbegriffe der biometrischen Systeme

Entscheiden Sie sich **bei jedem Begriff** für **eine** der vorgeschlagenen Definitionen und begründen Sie mit **zwei Sätzen**, warum Sie diese Definition gewählt haben. Es gibt eine oder mehr als eine richtige Definition pro Begriff, Sie können sich aber nur eine aussuchen.

(1) Biometrische Identifikation

a) ... ist der Abgleich vieler biometrischer Referenzmuster gegen ein biometrisches Merkmal.
b) ... ist ein Verfahren zur Ermittlung der Identität einer Person mittels eines Computersystems.
c) ... ist der Abgleich eines biometrischen Merkmals gegen ein anderes, das auf einer Karte oder in einer Datenbank gespeichert ist.

(2) Biometrische Verifikation

a) ... ist die Ersterfassung eines biometrischen Merkmals in einem System.
b) ... ist der Vergleich des aus einem Sample extrahierten Musters mit dem Template, das mit einem Namen oder einer User-ID hinterlegt wurde.
c) ... heißt auch Pattern Matching.

(3) Die Falschrückweisungsrate

a) ... gibt den Prozentsatz der Personen an, die fälschlicherweise keinen Zugang mithilfe eines biometrischen Systems bekommen haben, obwohl die jeweilige Person zugangsberechtigt war.
b) ... gibt den Prozentsatz der Personen an, deren Bilder nicht in das System eingepflegt werden konnten.
c) ... entspricht, wenn sie gleich der Falschakzeptanzrate ist, der Equal Error Rate eines biometrischen Systems.

Aufgabe 2 ..... [12 P/]

Komponenten und Prozesse eines biometrischen Systems

a) Schauen Sie sich das Schaubild in der **Anlage 1** an und benennen Sie die fehlenden Komponenten/Subsysteme oder Prozesse. Die fehlenden Begriffe sind mit einem Fragezeichen und einer Zahl markiert. (4 Punkte)

b) Erläutern Sie anschließend deren Funktion (nicht als Stichwort im Schaubild, sondern als Text auf dem vom Fachlehrer ausgeteilten Schreibpapier!). (8 Punkte)

Aufgabe 3 ..... [18 P/]

a) Lesen Sie zunächst **Anlage 2** und erklären Sie dann kurz, worum es sich bei *Eurodac* handelt. (6Punkte)

b) Nehmen Sie zu folgender Frage kritisch Stellung:

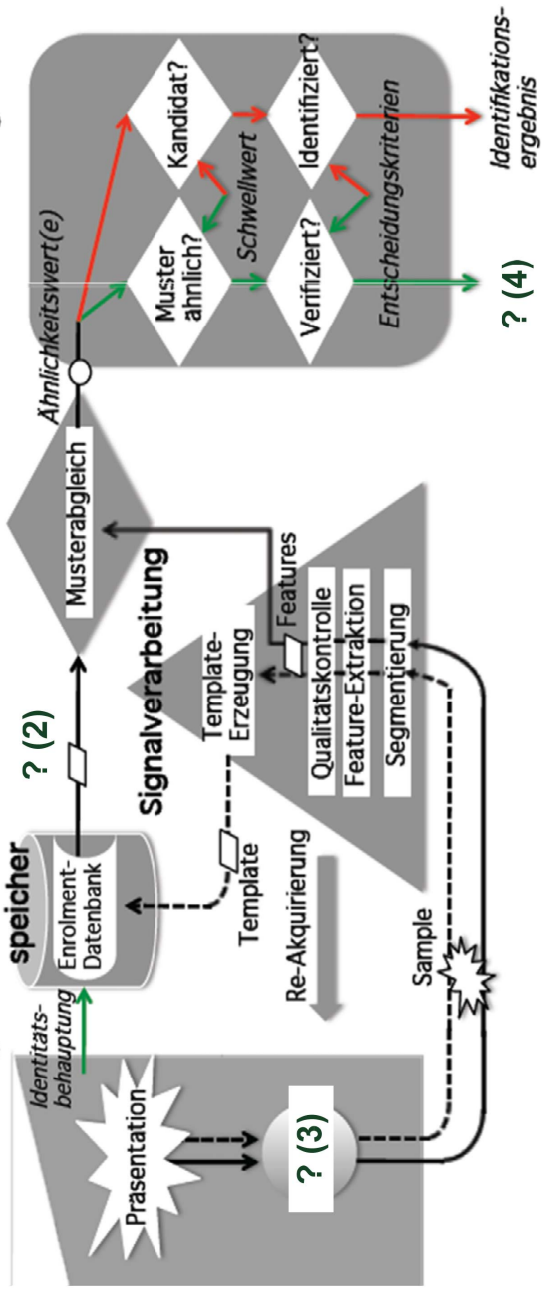
Ist der Einsatz einer biometrischen Technik wie Eurodac im Bereich der Migrationspolitik gerechtfertigt?

Stützen Sie Ihre Sichtweise mit aussagekräftigen Argumenten. (12 Punkte)

Klausuraufgabe OSZ Handel

Name: _____

Anlage 1: Generisches biometrisches System nach ISO-Norm 2006 (19795 -1)



Lösungen:

1) _____ 3 _____

2) _____ 4) _____

Klausuraufgabe OSZ Handel

Anlage 2

Ein Fallbeispiel der Biometrie: Die Rolle von Eurodac in der Asylpolitik Deutschlands

In der Rechtsprechung zu Asylverfahren in Deutschland kommt es in den letzten Jahren häufig zur Heranziehung der Daten des EU-weiten Fingerabdruckidentifizierungssystems Eurodac. Die Entscheidung des folgenden Beispielfalles ist noch offen und bereits durch mehrere gerichtliche Instanzen gelaufen:

Verpflichtung zur Abgabe verwertbarer Fingerabdrücke

Der Kläger stammt nach eigenen Angaben aus Somalia. Er gibt an, im März 2010 nach Deutschland eingereist zu sein und beantragte hier Asyl. Von ihm waren keine Fingerabdrücke zu erlangen, die für einen Datenabgleich über eventuell bereits durchgeführte anderweitige Asylverfahren (Eurodac-Anfrage) verwertbar waren. Daraufhin forderte ihn das Bundesamt für Migration und Flüchtlinge (Bundesamt) auf, das Asylverfahren dadurch zu betreiben, dass er verwertbare Fingerabdrücke abgebe. Nachdem auch die neuerlich abgegebenen Fingerabdrücke des Klägers als nicht verwertbar eingestuft wurden, stellte das Bundesamt mit Bescheid vom Oktober 2010 fest, dass der Asylantrag als zurückgenommen gilt, das Asylverfahren eingestellt ist, und dass Abschiebungsverbote nach § 60 Abs. 2 bis 7 Aufenthaltsgesetz nicht vorliegen. Dem Kläger wurde die Abschiebung in den Herkunftsstaat angedroht.

Die hiergegen erhobene Anfechtungsklage wies das Verwaltungsgericht ab. Der Bayerische Verwaltungsgerichtshof hat den Bescheid hingegen aufgehoben. Er hat die Voraussetzungen für das Nichtbetreiben des Verfahrens nach § 33 Abs. 1 Asylverfahrensgesetz (AsylVfG) nicht als erfüllt angesehen. Denn die vom Ausländer geforderte Mitwirkungshandlung finde im Gesetz keine hinreichende Stütze. Ein Ausländer sei nach § 15 Abs. 2 Nr. 7 AsylVfG zwar verpflichtet, an erkennungsdienstlichen Maßnahmen mitzuwirken. Eine Verpflichtung, Fingerabdrücke in verwertbarer Qualität abzugeben, bestehe indes nicht. Dies bedürfe einer ausdrücklichen gesetzgeberischen Entscheidung, an der es fehle. Hiergegen richtet sich die Revision des Bundesamtes.

BVerwG 10 C 12.11

QUELLE: Bundesverwaltungsgericht: Wichtige Entscheidungen im Jahr 2012. URL: http://www.bverwg.de/enid/Jahrespressegespraech_2_ss2/Rechtsprechungsvorschau_2_ss2_qc.html